

BREAKING &REMAKING LAW AND TECHNOLOGY:

A Socio-Techno-Legal Study of Hacking

Michael Anthony C. Dizon

**BREAKING AND REMAKING
LAW AND TECHNOLOGY**

A Socio-Techno-Legal Study of Hacking

MICHAEL ANTHONY C. DIZON

BREAKING AND REMAKING LAW AND TECHNOLOGY

A Socio-Techno-Legal Study of Hacking

Proefschrift

*ter verkrijging van de graad van doctor
aan Tilburg University opgezag van de rec-
tor magnificus, prof.dr. E.H.L. Aarts, in het
openbaar te verdedigen ten overstaan van een
door het college voor promoties aangewezen
commissie in de aula van de Universiteit op
dinsdag 28 juni 2016 om 16.15 uur door*

MICHAEL ANTHONY CO DIZON

geboren op 13 juni 1975

te Quezon City, Filipijnen

Promotores:

prof.dr. R.E. Leenes

prof.dr. E.J. Koops

Overige leden van de Promotiecommissie:

prof.dr. P.J.A. de Hert

prof.dr. N. Helberger

prof.dr. B.P.F. Jacobs

prof.dr. T. Swierstra

ACKNOWLEDGMENTS

Researching and writing this book would not have been possible without the help of the following persons, groups and institutions. I would like to extend my gratitude to them for their contribution and assistance in making this book: my supervisors, Professor Ronald Leenes and Professor Bert-Jaap Koops, for their guidance and feedback throughout the entire process; Tilburg University for granting me the opportunity to conduct this research as a PhD candidate; the faculty and staff of Tilburg Law School for their help and advice on academic and administrative matters; my colleagues at the Tilburg Institute for Law, Technology, and Society (TILT) for their camaraderie and useful comments on my research, particularly Dr Maurice Schellekens, Dr Bryce Newell and Dr Tjerk Timan for their detailed notes on specific chapters; the administrators and staff of the International Institute for the Sociology of Law for the grant to conduct research at their excellent library and documentation center; the organizers and students of Netherlands Graduate Research School of Science, Technology and Modern Culture (WTMC) Summer School 2014 for an informative week learning about science and technology studies; the faculty, staff and students of the Oxford Internet Institute's Summer Doctoral Programme 2015 for sharing their research and expertise with me; Val Datu and VJ Graphic Arts for the design and layout, and my family and friends for their encouragement and support. I would especially like to express my appreciation to the members of the Dutch hacker community for their openness and generosity in agreeing to interviews, chatting with me, listening and reacting to presentations about my research at hacker conferences, and allowing me to observe and participate at various hackerspaces and hacker events. I hope that I was able to capture the essence of hacker culture as much as possible and to see the world through your eyes. Most of all, I would like to thank my wife who is always with me every step of the way.

S U M M A R Y

In an increasingly digital and connected world, technological groups like hackers play a significant role in the workings and governance of society. This book examines the relations and interactions between hacking and the law by focusing on two types of hackers: makers, who are interested in hacking all kinds of technologies and regularly hang out at communal workshops called hackerspaces to build, share and collaborate on projects, and hacktivists, those who engage in hacking activities for overtly socio-political purposes. In this research, hacking is defined as the creative, innovative and unexpected use of technology. The central research question of the book is: In relation to their technologies, norms and values, how do makers and hacktivists interact with and respond to technology laws and policies? Since the research lies at the intersection of law, technology and society, the book adopts an interdisciplinary socio-techno-legal approach that combines the fields of technology law, science and technology studies, and socio-legal studies. With regard to methods, it utilizes doctrinal legal research together with various types of qualitative research methods. In addition to the legal analysis of laws that are relevant to hacking, empirical data about makers and hacktivists was collected through interviews, participant observation at hackerspaces and hacker events, and content analysis of hacker manifestos, and subsequently analyzed through a qualitative, inductive and interpretivist approach. The book aims to contribute to a better understanding of the legal and normative impact of hackers and to improve approaches to the regulation and governance of technology.

Makers and hacktivists are part of a longstanding and vibrant hacker culture that has its own distinguishing technologies, practices, norms and values. There are different types of hackers who preceded makers and hacktivists. They include the original computer hackers, computer hobbyists, underground hackers, and FOSS developers. Hacker culture and these previous hacker generations have a strong influence on makers and hacktivists. Like the other hacker types, makers and hacktivists are extremely passionate about technology and desire to use it in new and creative ways. Makers are

especially enthusiastic about continuing the hacker tradition of creatively using technology to produce inventions and other technical advances. There is also a rebellious and non-conformist streak that runs through all types of hackers. But while hacktivists share the same anti-establishment attitude and countercultural goals of early computer hackers and computer hobbyists, they do not consider technology as an end in itself but as a powerful means for socio-political ends.

With respect to their norms and values, makers and hacktivists share many things in common. The values of creativity and innovation, curiosity, and individual autonomy and liberty rank highest for both of them. Makers and hacktivists also place great importance on having free and open access to and use of information and technology. But there are differences between them as well. While they both highly prize community development and social development, makers place greater emphasis on the former and hacktivists the latter. Makers are also more concerned about the values of openness and transparency because they require full access to technologies and systems so they can use them in new and interesting ways. Hacktivists, on their part, consider privacy and security to be of utmost importance.

Computer crime, intellectual property, contract, and anti-circumvention rules and regulations are the laws that are most relevant to makers and hacktivists. What is common among these laws and what connects them to hacking is that, like hacking, they essentially deal with or concern access to and use of information and technology. Existing technology laws and policies tend to restrict rather than support makers and hacktivists. In general, computer crime laws are very broad and restrictive and over-criminalize hacking. Because of the vague and low legal thresholds for committing computer security crimes, many hacking activities, including those that are creative or innocuous, are subject to criminal prosecution. While intellectual property laws grant creators and inventors extensive rights over their creations, the corollary limitations and exceptions to these rights that could benefit hackers and ordinary users and preserve the intellectual property balance are few and far between. These problems are further exacerbated by the use of restrictive contracts and anti-circumvention technologies and rules that technically and

legally preclude potentially creative and innovative uses of protected information and technology. Despite these conflicts, it is curious to see how hacking and the law share and seek to protect and promote essentially the same social interests and goals. Like intellectual property laws, the main goal of hacking is to produce creative works and innovative technologies and make them available to the public. Protecting the security of computer systems and data, which is the primary objective of computer crime laws, is considered an important value as well among makers and hacktivists. While they may have serious differences, hacking and the law are connected on a fundamental level and, through these areas of connection and intersection, the tensions between them may be resolved.

The relations and interactions between hacking and law and public authorities can be characterized as complex and multifaceted. Makers' and hacktivists' general responses to law are: to ignore and avoid it; if it becomes impossible to keep the law away, to change or resist it; and, if it benefits the hacker community and society as a whole, to possibly work with, use or adapt the law. As seen in the campaign against electronic voting machines, hackers can strive to change technology laws and policies that they disagree with through technical means. But, they can also utilize or work within the legal system to change and improve laws, as demonstrated by the adoption of the net neutrality legislation in the Netherlands and the continued development and use of open source projects and licenses to counteract the restrictions and restrictive uses of intellectual property rights. Makers and hacktivists are also willing to work with public authorities if they believe that such projects or activities will have a social impact and redound to the benefit of their community and the wider public. Furthermore, even though makers and hacktivists may have problems with law and public authorities, they are surprisingly open to knowing more about the law, receiving greater legal protection for their fundamental rights and freedoms, and even ensuring the integrity of a system that elects public officials. This apparent incongruity can be explained by the fact that makers and hacktivists perceive and approach the law and authority in two distinct ways: restrictive or unjust laws and governments must be opposed, while laws and systems that uphold basic human rights and promote democratic freedoms and processes should be support-

ed.

Despite the complex and conflicting relations between hacking and the law and public authorities, their differences can be reconciled by building on their shared values, having a more open and empathetic view of and reaction to the other, and working as partners in the development of technology laws and policies. Makers and hacktivists should view public authorities as representatives of the demos and as public servants who strive to achieve the same liberal democratic goals. It would also be more productive if the law and public authorities perceived and treated hackers as co-participants or collaborators in the development of technology laws and policies. The responsible disclosure rules and open data hackathons are noteworthy examples of hackers and public authorities constructively working together. However, in order to meaningfully improve the laws that affect makers and hacktivists and to encourage the creativity and innovation that is inherent in hacking, existing computer crime, intellectual property and other relevant laws need to be improved. The recommended legal changes include: incorporating malicious or criminal intent as an essential element of computer security crimes; adopting the three-step test as an open-ended standard for determining the limitations and exceptions to intellectual property rights; introducing more limitations and exceptions to anti-circumvention rules; and prohibiting contractual waivers of limitations and exceptions to intellectual property rights.

Based on the empirical findings and socio-legal analysis of this book, technological actors like makers and hacktivists do indeed play a vital role in determining what rules regulate and govern the networked information society. It would be more productive then for the law and public authorities to treat makers and hacktivists not as regulatory threats and targets but as genuine co-participants or potential collaborators in the development of technology laws and policies. They should take into account hacker practices, norms and values when developing laws that impact hacking. Despite their general distrust of centralized authorities, makers and hacktivists should be more open and willing to assist and work with public authorities and share their knowledge and skills to improve or make better laws. This is particularly relevant given that makers' and hacktivists' primary criticism or complaint about public authorities is the latter's lack of in-depth technical knowledge and understanding of the underlying technologies and technical practices that are the objects of regulation. By building on their commonalities and having greater empathy for the other, the conflicts between hacking and the law can be potentially lessened or settled.

CONTENTS

CHAPTER ONE

Introduction: Hacking and law	17
1.1 Technological actors and governance of the networked society	17
1.2 Hackers	19
1.2.1 Hack	19
1.2.2 Makers	23
1.2.3 Hacktivists	24
1.3 Conceptual framework and research questions	26
1.4 Analytical framework	30
1.4.1 Common acts of hacking	30
1.4.2 Breaking and making	33
1.4.3 Norms and values	35
1.5 Methodology	37
1.5.1 Socio-techno-legal study	37
1.5.1.1 <i>Socio-legal studies</i>	38
1.5.1.2 <i>Science and technology studies</i>	39
1.5.1.3 <i>Technology law research</i>	40
1.5.2 Qualitative research	43
1.5.3 Inductive and interpretivist approach	45
1.6 Research methods	49
1.6.1 Data collection	49
1.6.2 Coding and analysis	55
1.7 Overview of chapters	59

CHAPTER TWO

Hacker culture	61
2.1 Histories and dimensions of hacking	61
2.2 A narrative typology of hackers	67
2.2.1 Of minicomputers and laboratories – Computer scientists and programmers	71
2.2.1.1 <i>The Hulking Giants</i>	71
2.2.1.2 <i>The TX-0</i>	72
2.2.1.3 <i>The PDP-1</i>	74
2.2.2 Of microcomputers, garages and computer clubs – Computer hobbyists	76
2.2.2.1 <i>The Altair</i>	76
2.2.2.2 <i>The Homebrew Computer Club</i>	79
2.2.2.3 <i>The Apple II</i>	82
2.2.2.4 <i>Blue boxes and paper tapes</i>	84
2.2.2.5 <i>Free and open versus proprietary and closed</i>	90
2.2.3 Of personal computers, modems and bedrooms – Underground hackers	92
2.2.3.1 <i>Bulletin Board Systems</i>	92
2.2.3.2 <i>The digital underground</i>	95

2.2.4	Of free and open source software, licenses and movements – FOSS developers	100
2.2.4.1	Free software	100
2.2.4.2	Copyleft	104
2.2.4.3	Linux	108
2.2.4.4	FOSS and other movements	110
2.2.5	Of the world wide web of computers and communities – Hacktivists	113
2.2.5.1	Hacklabs, hackmeets and hacker cons	113
2.2.5.2	Taking to the streets and the information superhighways	117
2.2.6	Of open technologies, projects and spaces – Makers	120
2.2.6.1	Open innovation	120
2.2.6.2	Hackerspaces	123
2.2.6.3	MakerBot	129
2.3	Makers and hacktivists in context	134

CHAPTER THREE

Hacker norms and values	137	
3.1	The why of hacking	137
3.2	Conceptual elaborations	138
3.2.1	Norms	138
3.2.2	Values	142
3.3	Manifestations of norms and values	144
3.3.1	Manifestos	144
3.3.2	Hacker manifestos	147
3.3.2.1	The Hacker Ethic	151
3.3.2.2	The Conscience of a Hacker	154
3.3.2.3	The GNU Manifesto	155
3.3.2.4	An Anonymous Manifesto	158
3.3.2.5	This is the Maker Manifesto	160
3.4	Norms and values of makers and hacktivists	162
3.4.1	Creativity and innovation	163
3.4.2	Curiosity	166
3.4.3	Individual autonomy and liberty	168
3.4.4	Community development	170
3.4.5	Social development	174
3.4.6	Other prominent norms and values	177
3.4.6.1	Openness and freedom of access	177
3.4.6.2	Transparency	180
3.4.6.3	Security	184
3.4.6.4	Privacy	187
3.5	Normatively full and value-laden	

4.1 A normative and axiological approach	196
4.2 Computer crime laws	198
4.2.1 Brief history and development	198
4.2.2 Computer crime and hacking	202
4.2.3 Illegal access	203
4.2.3.1 Access or entry without right	203
4.2.3.2 Objectives and justifications	206
4.2.3.3 Conflicts with acts, norms and values of hacking	208
4.2.3.4 Problem of overbreadth and vagueness	212
4.2.3.5 Unintended consequences and negative effects	214
4.2.3.6 Exploitable gaps, loopholes and contradictions	217
4.2.4. Illegal interception	219
4.2.4.1 Capture data transmissions and emissions	219
4.2.4.2 Legal and social justification	222
4.2.5 Data interference and system interference	223
4.2.5.1 Damage or hinder computer data and systems	223
4.2.5.2 Cyber attacks as a form of system interference	227
4.2.5.3 Lawful versus unlawful interference	229
4.2.6 Misuse of devices	238
4.3 Intellectual property laws	241
4.3.1 Fraught history of intellectual property and socio-technical innovation	241
4.3.2 Intellectual property balance	242
4.3.3 Broad exclusive rights yet narrow limitations and exceptions	248
4.3.3.1 Reverse engineering, decompilation and use of software	251
4.3.3.2 Temporary acts of reproduction	255
4.3.3.3 Private and non-commercial copying and use	257
4.3.3.4 Scientific research and teaching	259
4.3.3.5 Repair of equipment	261
4.3.3.6 Fair use and the three-step test	267
4.4 Contract and anti-circumvention laws	268
4.4.1 Contracts	268
4.4.1.1 Contractual terms and conditions	268
4.4.1.2 Freedom and restraints of contract	269
4.4.1.3 Contracts and computer crime	272
4.4.2 Anti-circumvention rules	276
4.4.2.1 Technological protection measures	276
4.4.2.2 Techno-legal barriers	281
4.5 Conflicts and correspondences between hacking and law	286

CHAPTER FIVE

Hacking's interactions with law	289
5.1 Perceptions and attitudes of hackers toward law and authority	289
5.1.1 Problem with authority	290
5.1.2 Trouble with the law	293
5.1.3 Legal and extra-legal means	298
5.1.4 Presence rather than the absence of law	302
5.1.5 Know the law more	304
5.1.6 Greater access to law and legal assistance	308
5.2 Hackers' responses to law	310
5.2.1 Ignore and avoid	311
5.2.2 Change and resist	314
5.2.2.1 Legal change through hacking	314
5.2.2.2 Hacking electronic voting computers	316
5.2.2.3 Leaktober	322
5.2.2.4 Hacking the OV-chipcard	325
5.2.3 Work with, use and adapt	331
5.2.3.1 Net neutrality rules	331
5.2.3.2 Open source projects	338
5.3 Complex relations and reactions	341

CHAPTER SIX

Normative conclusions and legal recommendations	345
6.1 Normative implications	345
6.1.1 Hackers as technical, social and legal actors	345
6.1.2 Resolving conflicts by building on commonalities	347
6.2 Support and reach out to hackers	349
6.2.1 Responsible disclosure	349
6.2.1.1 Responsible disclosure rules	349
6.2.1.2 <i>Hackers' reactions</i>	355
6.2.1.3 Changing attitudes, changing laws	358
6.2.2 Open data	361
6.2.2.1 Policies and initiatives	361
6.2.2.2 Hackathons	364
6.3 Change and improve the law	369
6.3.1 Computer crime laws	369
6.3.1.1 Hacking as a legitimate and common activity	369
6.3.1.2 Essential requirement of criminal intent	371
6.3.2 Intellectual property laws	376
6.3.2.1 Three-step test as akin to fair use	376
6.3.2.2 Three-step test plus	381
6.3.3 Anti-circumvention and contract laws	386
6.3.3.1 More limitations and exceptions to anti-circumvention	386
6.3.3.2 Necessary nexus between circumvention and copyright infringement	388

6.3.3.3 No contractual waivers of limitations and exceptions	391
6.3.4 Rights of users	392
6.4 Hacking can be change for good	396
CHAPTER SEVEN	
Epilogue: The value and future of socio-techno-legal studies	401
7.1 For law and policymaking	401
7.2 For law and technology research	406
APPENDIX A	
Interview guide	411
APPENDIX B	
Code List	415
BIBLIOGRAPHY	423

Introduction: Hacking and law

1.1 Technological actors and governance of the networked society

In today's digital, technical and connected world, technologists and technological groups (i.e., those primarily engaged in the creation, development, adoption, use, dissemination or control of information and communications technology) play an important role in the operations and governance of the "networked information society".¹ Increasingly, people's behaviors online and offline are influenced not only by states and governmental entities but also non-state actors and organizations. For instance, non-national and non-governmental entities and bodies that maintain the underlying protocols and technical architectures of computer networks such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN) influence what individuals and entities can or cannot do on the internet.² Similarly, innovators and technically proficient groups are able to help bring about or heighten profound changes in society. Free and open source software (FOSS) developer communities, for example, have served as models for greater openness and accessibility not just in software programming but also in the fields of education and content creation and distribution (e.g., Creative Commons and open access).³ Activists have successfully used digital technologies to pursue political and social ends,⁴ and the online groups Wikileaks

¹ Julie Cohen, *Configuring the Networked Self* 3; see Manuel Castells, *The Internet Galaxy* 133 (who uses the term "network society").

² See Andrew Murray, *The Regulation of Cyberspace* 74; see Kathy Bowrey, *Law and Internet Cultures* 47; see Jeanne Bonnici, *Self-Regulation in Cyberspace* 77.

³ See Christopher Kely, *Two Bits* 3.

⁴ Andrew Chadwick, *Internet Politics* 114.

and Anonymous have notoriously used their technical knowledge and skills to cause great disruption to political and technical systems to the embarrassment and dismay of governments and law enforcement bodies around the world.⁵

In light of the growing influence of these technological actors and groups on technical, social and legal matters, due in part to the increasing technologization of society,⁶ it is important for them, together with their norms, values and technologies, to be the subject of more in-depth study in the field of technology law. There is one particular technological group that has been very influential in advancing digital technologies and shaping culture since the late 1950s – hackers. From the early computer scientists and programmers at the Massachusetts Institute of Technology (MIT) who first used “hacker” as a self-referential term,⁷ and through the succeeding generations of hackers – computer hobbyists (1970s), underground hackers (1980s to present), FOSS developers (1980s to present), hacktivists (1990s to present) and makers (1990s to present) – hackers can and do shape law, technology and society in new and interesting ways.⁸ Given that hacking has both technical and normative effects on society, it is crucial to discover and analyze what the practices, norms and values of hackers are and how do they interact and come into conflict with the law, which is generally considered to be the principal means by which individual and social behavior is controlled and regulated.

Of the many types of hackers, makers and hacktivists deserve more attention and require further research because: first, they have been receiving increasing public and media attention because of their innovative and disruptive technologies and activities; second, they

⁵ Peter Ludlow, “Wikileaks and Hacktivist Culture” 25; Noah Hampson, “Hacktivism” 512-513.

⁶ Patrice Flichy, *Understanding Technological Innovation* 17; Raul Perterra, “The Anthropology of New Media in the Philippines” 16.

⁷ Paul Taylor, *Hackers* 13;

⁸ For more information on the different generations and types of hackers, see Steven Levy, *Hackers*; see Paul Taylor, “Editorial: Hacktivism”; see Kirsty Best, “The Hacker’s Challenge” 266-267; see E. Gabriella Coleman and Alex Golub, “Hacker practice”; see Helen Nissenbaum, “Hackers and the contested ontology of cyberspace”; Paul Taylor, “From hackers to hacktivists” 628-629 (who lists seven hacker generations).

represent two ends of hacker culture (one that is focused primarily on technological creation and the other on socio-political disruption); and finally, they influence and are similarly affected by the two laws that are most pertinent to hacking, namely, computer crime and intellectual property laws. Through their technical projects and acts of hacktivism, makers and hacktivists are pushing not just technical but legal and social boundaries as well. Makers and hacktivists are similar in that they both engage in hacking activities in public. Makers are members of hackerspaces, which have open memberships and where hacking is done out in the open with most projects being documented and freely shared online. Similarly, hacking activities carried out by hacktivists are meant to raise public awareness and catalyze social action about important public interest issues. While their activities can be veiled in secrecy and anonymity, hacktivists ultimately seek to make a public impact. The makers and hacktivists I met know each other and they attend some of the same hacker events. Several hacktivists are also members of hackerspaces and a number of makers take part in hacktivist campaigns. There is thus a close connection between makers and hacktivists in the Netherlands.

1.2 Hackers

1.2.1 HACK

The term “hacker” has been used to define and describe different individuals and groups. However, since there is not one but many types of hackers, it is difficult to come up with a single, universal definition that encompasses all of them. Even the meaning of “to hack” in relation to computers and technologies is contested and has been constantly evolving since it was first used in connection with the activities

of the MIT computer hackers.⁹ According to *The New Hacker's Dictionary*, a hack is characterized by “an appropriate application of ingenuity” to any field of activity.¹⁰ For Levy, a hack “must be imbued with innovation, style, and technical virtuosity”.¹¹ To Jordan, a “hack involves altering a pre-existing situation to produce something new; to hack is to produce differences”.¹² Organizers of a hacker camp define hacking as “to use something in a creative way, not thought of when it was first invented”.¹³ Of the many descriptions of hacking, Turkle's characterization of the hack, which she first wrote in 1984, remains the most relevant, flexible and useful since, despite its high level of conceptualization, it is applicable to most types of hackers and hacking activities. She expounds on the meaning of hacking through the activities of the well-known hacker John Draper (Captain Crunch) who, using a whistle and his knowledge of the intricacies of the global telephone system, was able to make a free long-distance telephone call that “started in California, went through Tokyo, India, Greece, Pretoria, London, New York, and back to California”.¹⁴

Appreciating what made the call around the world a great hack is an exercise in hacker aesthetics. It has the quality of Howard's magician's gesture: a surprising result produced with what hackers would describe as ‘a ridiculously simple’ means. Of equal importance to the aesthetic of the hack is that Crunch had not simply stumbled on a curiosity. The trick worked because Crunch had acquired an impressive amount of expertise of the telephone system. This is what made the trick a great hack, otherwise it would have been a minor one. Mastery is of the essence everywhere within hacker culture. Third, the expertise was acquired unofficially and at the expense of a big system. The hacker is a person outside the system who is never excluded by its rules.¹⁵

⁹ “The Meaning of ‘Hack’”, *The New Hacker's Dictionary*; Paul Taylor, *Hackers* 13.

¹⁰ “The Meaning of ‘Hack’”, *The New Hacker's Dictionary*.

¹¹ Steven Levy, *Hackers* 10.

¹² Tim Jordan, *Hacking 9*; see also Tim Jordan, *Activism!* 120 (a hack is the “innovative” and “novel uses of technology”).

¹³ OHM2013, “Call for Participation”.

¹⁴ Sherry Turkle, *The Second Self* 207.

¹⁵ Sherry Turkle, *The Second Self* 208.

To paraphrase and refine the above quote from Turkle, whether as noun or verb, a hack is about producing innovation through deceptively simple means, which belies the impressive mastery or expertise possessed by an actor who does not conform to the normal rules and expected uses of a technology or technical system.¹⁶ Hacking is basically the creative, innovative and unexpected use of technology. A hack, whether as product or process, is innovative because it is either new, novel, different or surprising. A hack's deceptive simplicity tends to make it appear magical.¹⁷ In my refined characterization of a hack, expertise can but does not have to be acquired unofficially or at the expense of a big system; the key is that a hack does not conform to the normal rules or expected uses of a technology. As Taylor states, "true' hacking is in the system but not of the system, and to remain true to itself it remains dependent upon, but not beholden, to that system".¹⁸ Thus, the elements of a hack are (1) innovation, (2) simplicity, (3) mastery, (4) non-conformity, and (5) technology.¹⁹

Despite the plurality of hackers and the various meanings attached to the word "hack", taken together, the multiplicity of actors, activities and meanings constitutes a loosely joined but distinct hacker culture. This culture is generally concerned with hacking technologies, particularly those pertaining to computing and communication, and espouses common yet contested norms and values such as, among others, openness, freedom of access, freedom of expression, autonomy, equality/meritocracy, transparency, and privacy.²⁰ Because it originated from the early computer hackers at MIT, hacker culture is closely connected to different forms of computer culture and may be consid-

¹⁶ Sherry Turkle, *The Second Self* 208.

¹⁷ Chris Anderson, *Makers* 82 (Arthur C. Clarke's famous quote: "any sufficiently advanced technology is indistinguishable from magic"); see also Lawrence Principe, "Renaissance Natural Magic" in *History of Science: Antiquity to 1700* (the connection between magic and natural philosophy).

¹⁸ Paul Taylor, "From hackers to hacktivists" 633.

¹⁹ Sherry Turkle, *The Second Self* 208; see Paul Taylor, *Hackers* 14 (who sees the three main characteristics of a hack as simplicity, mastery and illicitness); see Paul Taylor, "From hackers to hacktivists" (for his three core elements of the hacking ethic).

²⁰ Gabriella Coleman, "Hacker politics and publics" 513-514. These common norms and values can even be contested, paradoxically, to the point of negation.

ered the latter's progenitor.²¹ Hacking though is always at the forefront or the bleeding edge of technology creation and adoption. In the case of the MIT hackers, since computing was still a nascent field in the 1960s, the mere act of computer programming and finding ways to make computers do basic things like play music or display images was innovative.²² However, by the time computer hardware and software were commercialized and commoditized in the 1980s, hackers were no longer interested in just writing software or designing personal computers, but in exploring, learning about and hacking even more interesting and challenging technologies and technical systems such as online Bulletin Board Systems (BBS) and computer and telecommunications networks.²³ Computers are an important part of hacker culture, but hacking is not reducible to computers. Hacking involves pushing the limits of any technology and breaking the prescribed boundaries of all sorts of technical systems. The fact that hackers create and change technology is what separates them from individuals and groups who merely use or are enthusiastic about technology. Innovation, mastery and non-conformity are the elements that distinguish hacker culture from other technological cultures (e.g., gamer culture and cyberpunks).²⁴ Hackers are constantly innovating and pursuing new technological projects so that they can produce something new and surprise themselves and others. While this book's main focus is on makers and hacktivists, the other types of hackers that make up the broader hacker culture remain relevant to the analysis of hacking's relationship to technology law and policy. Hacker culture and the different hacker types are discussed in greater detail in Chapter 2.

²¹ Steven Levy, *Hackers* x; Eric Raymond, "A Brief History of Hackerdom" 4.

²² "PDP-1 Restoration Project", Computer History Museum; see also Pekka Himanen, "A Brief History of Computer Hackerism" 186. (note: not in bibliography)

²³ See Tim Jordan, *Hacking* 37.

²⁴ See Paul Taylor, *Hackers* xv; Douglas Thomas, *Hacker Culture* xii; Bruce Sterling, *The Hacker Crackdown* 59.

1.2.2 MAKERS

Makers are a particular type of hacker who are interested in hacking all kinds of technologies (even IKEA furniture)²⁵ and they regularly hang out at communal workshops called “hackerspaces” to build, share and collaborate on projects.²⁶ Makers had their beginnings in Europe and the United States in the 1990s, but they only began to be recognized and referred to by that name by the mid to late 2000s.²⁷ Hackerspaces are “places in the community where local [hackers] can collectively meet, work, and share infrastructure”.²⁸ The MakerBot 3D printer, the Pebble smart watch, the Square mobile payment system, and the user-sharing website Pinterest are some of the innovative products and services that were developed in hackerspaces.²⁹ Makers serve as an interesting case study of the interactions among laws, norms, values and technologies since they are at the forefront of exploring, developing and popularizing cutting-edge technologies such as 3D printers and autonomous drones that are expected to be legally, socially and economically disruptive. 3D printers are machines that can “print out” digital 3D objects or computer files as physical objects (normally made of plastic).³⁰ Once 3D printers are mass-produced and become a common household appliance, Anderson predicts that they will usher a “new industrial revolution” where ordinary people are able to create and produce almost anything in the comfort of their homes.³¹ 3D printing could be as legally challenging for the manufacturing industry as the photocopier was to the publishing industry and online peer-to-peer (P2P) file sharing technology was to the music industry.³²

²⁵ IKEA hackers <<http://www.ikeahackers.net/>> accessed 16 August 2013.

²⁶ Hackerspaces.org <<http://hackerspaces.org/wiki/>> accessed on 15 August 2013; see Andrew Schrok, “What Keeps Hacker and Maker Spaces Going?”.

²⁷ Hackerspaces - The Beginning 84.

²⁸ John Borland, “Hacker space’ movement sought for U.S.” *Wired.com*; see also Hackerspace Open Day <<https://revspace.nl/HackerspaceDagEn2012/>> accessed on 27 March 2013.

²⁹ Artisan’s Asylum, “Make a Makerspace”; Steven Kurutz, “One Big Workbench”.

³⁰ Chris Anderson, *Makers* 82.

³¹ Chris Anderson, *Makers* 41.

³² See Simon Bradshaw, Adrian Bowyer and Patrick Haufe, “The Intellectual Property Implications of Low-Cost 3D printing”; see Leanne Wiseman, “Beyond the Photocopier”; see Sudip Bhattacharjee and others, “Impact of Legal Threats on Online Music Sharing Activity”.

Makers share an affinity with computer hobbyists in the United States in the 1970s that were part of so-called homebrew computer clubs, which is considered the birthplace of the personal computing revolution.³³ Computer hobbyists hacked in relative isolation in their own garages and went to club meetings, which were held in different locations, to show off their creations to others.³⁴ Unlike makers, club members did not have access to more or less permanent and open places containing tools and equipment where people could work side-by-side on projects or just stay and hang out – in other words, a combined laboratory and living room. The connections between makers and computer hobbyists are discussed in more detail in Chapter 2.

1.2.3 HACKTIVISTS

In contrast to makers, hacktivists are those who hack for overtly socio-political purposes.³⁵ While all and even basic acts of hacking are political and socially relevant, overt intent is what distinguishes hacktivists from other types of hackers.³⁶ As Coleman explains, “In many other instances, geeks and hackers have no desire to act politically, even going as far as to disavow politics, but the technology they make and configure embodies values, and thus acts politically”.³⁸ The emergence in the 1990s of the term “hacktivists” to refer to socially and politically motivated hackers came about as a result of the confluence of a number of factors – globalization and the awareness of its effects, greater and widespread use of computers and the internet by activists as well as the wider public, and hackers themselves becoming more politically aware and involved.³⁸

³³ Steven Levy, *Hackers* 201 and 259; Robert Cringely, *Accidental Empires* 9.

³⁴ Steven Levy, *Hackers* 212, 214 and 216.

³⁵ See Paul Taylor, “Editorial: Hacktivism” 2 (who also uses the term overt); Paul Taylor, “From hackers to hacktivists” 626; see also Xiang Li, “Hacktivism and the First Amendment” 302 and 305; see also Noah Hampson, “Hacktivism” 514.

³⁶ Brian Alleyne, “We are all hackers now” 24 (who says “all hackers are political actors”); Tim Jordan, *Activism!* 135.

³⁷ Gabriella Coleman, “Hacker politics and publics” 516.

³⁸ Paul Taylor, “Editorial hacktivism” 5; Paul Taylor, “From hackers to hacktivists” 67; Tim Jordan, *Hacking* 71; Xiang Li, “Hacktivism and the First Amendment” 303.

While the term “hacktivism” is a simple contraction of the words hack and activism, it is closely related to but distinct from broader forms of cyber-activism, cyber-protests and other types of technology-based activism carried out by traditional activists.³⁹ What distinguishes hacktivism from general cyber-activism is that the former is grounded in, draws from, or views itself as a part of hacker culture, while the latter can but does not have to.⁴⁰ Furthermore, for hacktivists, the act of hacking itself constitutes both the form (expression and means) and the substance (content and message) of their activism – simultaneously a means and an end.⁴¹ In this way, the oft-cited Zapatista movement of the 1990s, where an indigenous community and their supporters used the internet to publicize and further their socio-political objectives, can be categorized as cyber-activism rather than hacktivism, even though some elements of the cyber-protest involved acts of hacking by hacktivists who were part of the movement.⁴²

Hacktivism can be carried out in different forms depending on the type of technology involved.⁴³ It can take the form of innocuous awareness campaigns and online self-organization, simple website defacement and site redirects, or of more forceful and direct actions such as a distributed denial-of-service attack (DDoS) against the web servers of the target entity or breaking the security of the target’s computer system.⁴⁴ A number of actions committed by hacktivists would be considered violations of different computer crime laws around the world. The controversy surrounding the whistleblower website Wikileaks and the many high-profile hacks and data breaches committed in its wake by online hacktivist groups such as Anonymous and LulzSec against governmental agencies and companies that they perceived to be op-

³⁹ Stefania Milan and Arne Hintz, “Dynamics of cyberactivism” 2; Noah Hampson, “Hacktivism” 515; Brian Alleyne, “We are all hackers now” 11.

⁴⁰ Brian Alleyne, “We are all hackers now” 11; Andrew Chadwick, *Internet Politics* 129-130.

⁴¹ Paul Taylor, “From hackers to hacktivists” 626; Noah Hampson, “Hacktivism” 531 (who argues that some forms of hacktivism are primarily expressive).

⁴² See Andrew Chadwick, *Internet Politics* 131-132; Paul Taylor, “From hackers to hacktivists” 634.

⁴³ Noah Hampson, “Hacktivism” 517; David Gunkel, “Editorial: introduction to hacking and hacktivism” 595.

⁴⁴ See Noah Hampson, “Hacktivism” 1 (for a list of different forms of hacktivisms); see Andrew Chadwick, *Internet Politics* 130.

pressive and undemocratic have brought hacktivism into the public eye.⁴⁵ Concerns about cyber attacks in Europe have led to proposals for greater, stronger and stricter state and stronger regulation.⁴⁶ The intensifying conflicts between hacktivists and state actors point to a potentially rich subject area of research since they too concern the interactions among different laws, norms, values and technologies.

1.3 Conceptual framework and research questions

Undoubtedly, studying makers and hacktivists and how they interact with technology laws and policies can contribute to a better understanding of who and what governs the networked society. Building on and refining Lessig's theory of the four modalities of regulation (law, social norms, the market, and architecture),⁴⁷ this book specifically focuses on the technologies, norms and values of makers and hacktivists and how they respond to the enactment and enforcement of technology laws. In lieu of "architecture" or "code" that Lessig employs for his fourth regulatory modality, I use "technology" since the latter term represents the main area of my research and it is broad enough to subsume the former two terms within its ambit. Technology is the "application of knowledge to production from the material world. Technology involves the creation of ... instruments (such as machines) used in human interaction with nature".⁴⁸ Technology should be understood a bit more broadly to also cover its corollary, science, as well as other practices and processes that involve the production and application of technical-scientific knowledge – i.e., both *techne* and *episteme*. I concur with the importance that Lessig places on "social norms", but I prefer to use the concept of "social field", which Moore

⁴⁵ Xiang Li, "Hacktivism and the First Amendment" 303; see also Parmy Olson, *We Are Anonymous*.

⁴⁶ "Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA", COM(2010) 517.

⁴⁷ Lawrence Lessig, *Code* 123.

⁴⁸ Anthony Giddens, *Sociology* 1135; see also Bert-Jaap Koops, "Ten dimensions of technology regulation" (who defines technology as "the broad range of tools and crafts that people use to change or adapt to their environment") 312.

describes as having its “own customs and rules and the means of coercing or inducing compliance”.⁴⁹ According to Bourdieu, “a field is a separate social universe having its own laws of functioning independent of those of politics and the economy”.⁵⁰ It “is organized around a body of internal protocols and assumptions, characteristic behaviors and self-sustaining values”.⁵¹ For Moore, a “social field is defined and its boundaries identified not by its organization... but by a processual characteristic, the fact that it can generate rules and coerce or induce compliance to them”.⁵² A social field thus encompasses social norms and other key sociological elements and concepts examined in this book, most specifically the social values, practices, beliefs, and processes of meaning-making of a specific group or community. With respect to “the market”, it is undoubtedly an important concept for certain kinds of research. However, since the focus of this book is on a particular social group (hackers) rather than a market, it neither aims nor requires the undertaking of economic research.

This book’s conceptual framework is therefore comprised of three domains that are principally concerned with the regulation and governance of the networked society – the legal, the social, and the technological (see Figure 1.1).⁵³ Each domain is distinct, yet they stand intimately close to one another. They possess common margins, which are porous, constantly ebbing and flowing, and always reshaping. But these shared borders are not so much barriers separating the domains, as they are areas of interaction, contact and osmosis. These boundary areas are thus crucial sites of mutual shaping and influence between the domains, as well as among the many individuals, groups, institutions and techno-social fields that they encompass. Furthermore, each

⁴⁹ Sally Falk Moore, “Law and Social Change” 721.

⁵⁰ Pierre Bourdieu, *The Field of Cultural Production* 162.

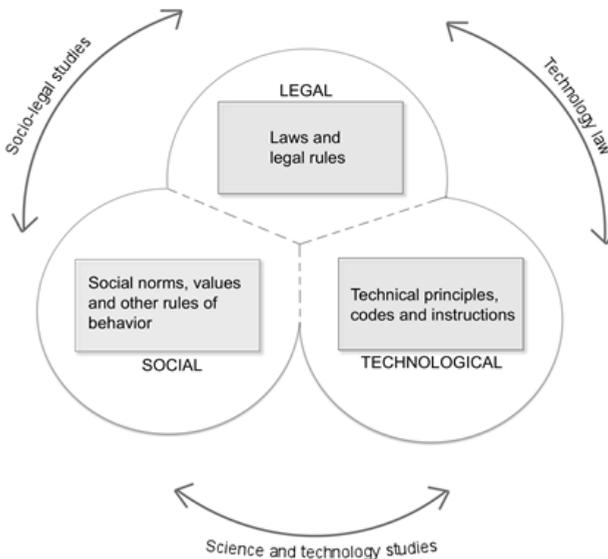
⁵¹ Richard Terdiman, “Translator’s Introduction” 806; see also Pierre Bourdieu, “The Force of Law: Toward a Sociology of the Juridical Field”.

⁵² Sally Falk Moore, “Law and Social Change” 722.

⁵³ See Michael Dizon, “Rules of a networked society” (for a more thorough and detailed explication of my theoretical approach to technology law research).

domain can be described in terms of the rules that constitute them. The legal domain can be conceived of as being made up of laws and legal rules; the social domain is permeated with social norms, values and other rules and standards of behavior; and the technological domain consists of technical-scientific principles, codes and instructions on how to produce and apply knowledge.⁵⁴ The relations and interactions between and among these three domains can be observed and analyzed using the socio-techno-legal approach advanced in this book. As illustrated in Figure 1.1, the relationship between the social and the legal can be examined using socio-legal studies; science and technology studies (STS) can help explain the relations between the technological and the social; and the interactions between the legal and the technological are within the purview of technology law. Section 1.5.1 below describes this social-techno-legal approach in greater detail.

Figure 1.1 Conceptual framework – Three domains principally concerned with the regulation and governance of the networked society.



⁵⁴ See Michael Dizon, “Rules of a networked society” 84-85.

Using the above conceptual framework, this book seeks to answer the central research question: In relation to their technologies, norms and values, how do makers and hacktivists interact with and respond to technology laws and policies? In discussing the central question, the following sub-questions are analyzed:

1. Who are makers and hacktivists and how are they connected to the broader hacker culture and other types of hackers?
2. What are the practices, technologies, norms and values of makers and hacktivists?
3. What laws and policies are specifically applicable or relevant to makers and hacktivists? How do the law and public authorities respond to hacking? How and to what extent do they tend to restrict and/or support hacking?
4. How do makers and hacktivists perceive, understand and respond to technology laws and policies? To what extent are these laws and policies accepted, disputed or negotiated? What forms do these responses take?
5. What is the significance of studying the relations between hacking and law? What can a socio-techno-legal approach and the research findings contribute to improving technology laws and policies concerning hackers?

1.4 Analytical framework

1.4.1 COMMON ACTS OF HACKING

Makers and hacktivists are multifaceted and they are part of and are subject to equally complex and heterogeneous contexts and conditions. The multiplicity that characterizes hacker culture poses a challenge to coming up with a systematic yet flexible research framework. In order to get a handle on the complex phenomena and issues involved, it is necessary to focus first on the hack. Even though hackers come from diverse socio-economic backgrounds and have various motivations and beliefs, by focusing on what hackers actually do, it becomes possible to distill further commonalities and connections among them.

As Taylor points out, the activity of hacking itself has not fundamentally changed; what has changed are the technological and social conditions within which hacking takes place.⁵⁵ Alleyne observes, for example, that the supposedly highly contentious ideological gap between free software developers and open source programmers recedes from view during the actual practice of hacking when both groups start creating “essentially the same object – source code, and [undertake the same] practice – code-sharing”.⁵⁶ As Kelty explains, “for all the ideological distinctions at the level of discourse, [free software and open source] are doing exactly the same thing at the level of practice”.⁵⁷ This does not mean that the substantial differences among the different types of hackers can be disregarded. Far from it, once a secure handhold is established by focusing initially on hacking activities, it becomes possible to undertake further analysis of the complexity of hacker culture and the plural norms and values that are associated

⁵⁵ Paul Taylor, “Editorial: Hacktivism” 2.

⁵⁶ Brian Alleyne, “We are all hackers now” 20.

⁵⁷ Christopher Kelty, *Two Bits* 14.

with it.

Because hacking is so semantically and culturally dense, using common everyday words to describe what a hack involves can help demystify it. Shorn of all its contested baggage (for the time being only),⁵⁸ hacking can be perceived as six common (in the sense of being both ordinary and shared) acts – (1) explore, (2) break, (3) learn, (4) create, (5) share, and (6) secure. The six common acts are derived and synthesized from some of the most well known expressions of the components and characteristics of hacker culture as written by hackers themselves and by non-hackers interested in hacker culture. The following acts of hacking are found in Levy’s famous codification of the hacker ethic – access, teach, set free, mistrust authority, decentralize, create, and change.⁵⁹ To Levy’s list, the German hacker group Chaos Computer Club appended the activities: make public data available and protect private data.⁶⁰ These actions are evident in Himanen’s seven values of the hacker ethic – pursue passions, make free, create something (valuable for the community), keep open, take action, care (for others), and create.⁶¹ From the four software freedoms advocated by FOSS hackers, the following acts can be gleaned: run, study (how the program works), change, access, redistribute, help (your neighbor), distribute (modified versions), and give (to the whole community).⁶² The preceding acts are related to core practices of free software: share (source code), keep open, coordinate, and collaborate.⁶³ In the maker movement, the following verbs are considered essential: make, share, give, learn, tool up, play, participate, support and change.⁶⁴ With respect to the related activities under each of the common acts, these are closely related acts that I came across during my research, readings and observations on hacker culture.

⁵⁸ See Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 44.

⁵⁹ Steven Levy, *Hackers* 28-31.

⁶⁰ Chaos Computer Club, “Hacker Ethics” <<http://www.ccc.de/hackerethics>> accessed 17 July 2013.

⁶¹ Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age* (Secker & Warburg 2001) 139-141.

⁶² Free Software Foundation, Inc., “What is free software” <<http://www.gnu.org/philosophy/free-sw.html>> accessed 7 November 2012.

⁶³ Christopher Kely, *Two Bits* 14-15.

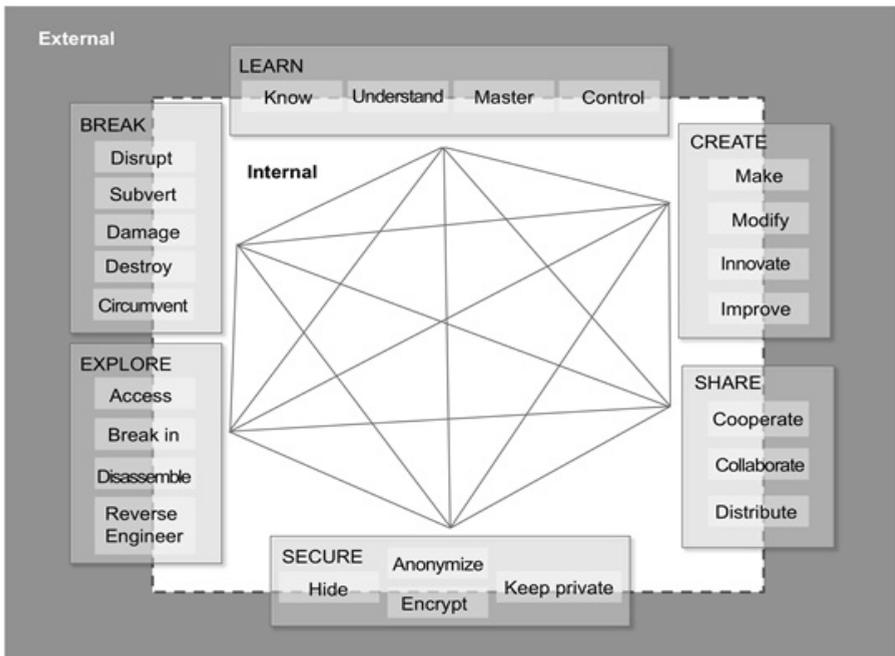
⁶⁴ Mark Hatch, *The Maker Movement Manifesto* 1-2.

The common acts can be imagined and represented as boxes containing more boxes (see Figure 1.2). The act to “explore” includes the related activities of access, break in, disassemble and reverse engineer; while “break” is further comprised of the acts disrupt, subvert, circumvent, damage and destroy. Other common acts also consist of various other activities – “learn” (know, master, control and understand), “create” (make, modify, improve and innovate), “share” (cooperate, collaborate and distribute), and “secure” (keep private, hide, encrypt and anonymize). These common acts are interconnected (as depicted by the crisscrossing lines between the different boxes) and there is no predefined path in their interactions since these can take place in all directions and in any order. For example, breaking can lead to learning but it can also produce sharing or creating (and the latter can lead back to learning).

The value of perceiving hacking as being made up of six common yet interacting acts is that one is able to peer into how hacking actually operates and how it impacts law, technology and society. I argue that the common acts of hacking and their interactions constitute the core engine that recursively animates and drives the technology, norm-making and value-forming practices and processes of makers and hacktivists. In Figure 1.2, the boxes representing the common acts straddle both the external and internal domains of hacker groups.⁶⁵ In this way, the common acts also serve as important means or mechanisms by which internal norms and values and technologies of hacker groups interact with external laws, and vice versa. It is also worth noting that the boundary between internal and external is generally nebulous and permeable so interactions can take place across the domains even without, but most especially through, hacking. The common acts of hacking, the theme of breaking and making, and the concepts of norms and values (discussed below) are meant to be an analytical guide to this book. The analytical framework can be valuable to other studies and future research on hackers and hacking.

⁶⁵ See Paul Taylor, “From hackers to hacktivists” 637 (who speaks of “the inside/outside issue faced by the hacker”).

Figure 1.2 Analytical Framework



1.4.2 BREAKING AND MAKING

By focusing on the common hacking activities and their interactivity, one becomes cognizant of the paradoxical “creative-destructive” dynamic that is inherent in hacking. Hackers generally want to learn how things work, gain expertise and produce something innovative, new or surprising. However, to understand and master a particular technology, hackers need to be able to access or glimpse its inner workings. But since most technologies and systems are closed or sealed off (black boxes), hackers need to take them apart or break into them. Breaking and making is a pivotal theme that is present throughout the development and evolution of digital technologies vis-à-vis hacker culture. The history of computing and hacking is replete with seemingly contradictory conditions and outcomes that arise from the interactions between creation and destruction. No less than Alan Turing, who is considered one of the fathers of computers and computer

science, was involved in the World War II computing and code-breaking efforts at Bletchley Park.⁶⁶ One of the first digital, stored-program computers, the Institute for Advanced Study (IAS) machine at Princeton, which was spearheaded by John von Neumann (who is credited with the eponymous computer architecture that is at the heart of many modern digital computers), was used to perform the calculations necessary for building a hydrogen bomb.⁶⁷ The internet's precursor, the ARPANET, was built to enable academics and researchers to connect remotely to computers and other users and share computing resources and information.⁶⁸ However, since it was funded and built under the auspices of the United States Department of Defense's Advanced Research Projects Agency (ARPA), it can be classified as military-related work produced by the military-industrial complex during the Cold War.⁶⁹ This may explain why the myth that the internet was made to survive a nuclear war still persists today.⁷⁰ Even hacker culture itself, which initially grew out of the activities of the early computer hackers at MIT, is suffused with the paradox of breaking and making – autonomy/control, anarchy/power, openness/secretcy and war/peace. As Levy points out, “ARPA money was the lifeblood of the hacking way of life” in the hacker utopia-dystopia on the ninth floor of Tech Square and “all the lab’s activities, even the most zany or anarchistic manifestations of the Hacker Ethic, had been funded by the Department of Defense”.⁷¹

Hacking is indeed a study in contradictions, and it is its magical ability to negotiate and bring together diametrically opposed forces and conditions that demonstrates its profound significance to law, technology and society. I argue that, like the natural philosophers,

⁶⁶ Douglas Thomas, *Hacker Culture* 13.

⁶⁷ See George Dyson, *Turing's Cathedral*.

⁶⁸ See Katie Hafner, *Where Wizards Stay Up Late* 41-42.

⁶⁹ See Katie Hafner, *Where Wizards Stay Up Late* 41-42.

⁷⁰ Internet Society, “Brief History of the Internet” (see footnote 5); see John Naughton, *A Brief History of the Future* 96-98; but see Michael Belliore, *The Department of Mad Scientists*.

⁷¹ Steven Levy, *Hackers* 125.

mathematicians, scientists, inventors and other innovators that preceded them, hackers occupy an extraordinary position since they are among the handful of social actors or groups that reside right at the nexus of the legal, social and technological domains.⁷² Being both technical and epistemic communities,⁷³ hacker groups influence how the networked information society is configured and operates through their tools, norms and values. The study of hackers and hacking therefore is relevant to understanding the techno-social changes and consequent legal challenges that society faces.

1.4.3 NORMS AND VALUES

Social norms and values are the primary conceptual and empirical foci of this book. A social norm (or norms for short) generally involves “(1) a collective evaluation of behavior in terms of what it ought to be; (2) a collective expectation as to what behavior will be; and/or (3) particular reactions to behavior, including attempts to apply sanctions or otherwise induce a particular kind of conduct”.⁷⁴ For its part, a value “is a conception, explicit or implicit, distinctive of an individual or characteristic of a group, of the desirable which influences the selection from available modes, means, and ends of action”.⁷⁵ Norms and values have always been the subject of legal scholarship (mainly in the form of law and society research), but they were only “rediscovered” in a big way by mostly law and economics scholars in the 1990s.⁷⁶ Placing greater attention and emphasis on these two concepts in their research has been appealing to legal scholars in general since laws, norms and values all concern and involve social relations and social order.⁷⁷ All three correlative concepts intrinsically “deal with norma-

⁷² See Wiebe Bijker, Thomas Hughes and Trevor Pinch, *The Social Construction of Technological Systems*.

⁷³ See Kasper Edwards, “Epistemic Communities, Situated Learning and Open Source Software Development” http://orbit.dtu.dk/fedora/objects/orbit:51813/datastreams/file_2976336/content accessed 8 November 2012.

⁷⁴ Jack Gibbs, “Norms: The Problem of Definition and Classification” 589 and 594.

⁷⁵ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 395.

⁷⁶ Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 157-158; see also Michael Hechter and Karl-Dieter Opp, *Social Norms* xii; Robert Ellickson, “The Evolution of Social Norms” 35; see also Richard McAdams and Eric Rasmusen, “Norms and the Law” 1609.

tive phenomena, [whether] partially or wholly”.⁷⁸ In addition to incorporating norms and values in their conceptual and analytical frameworks, there have been increasing calls for legal scholars themselves to “undertake primary research on norms”.⁷⁹ More than any other time, “there is a now greater appreciation of the need for empirical research to verify a law’s influence” on norms, and vice versa.⁸⁰ Ellickson’s book *Order without Law*, which is based on the author’s own empirical study of cattle ranchers and farm owners in the United States and their private norms on dispute resolution concerning animal trespass and damage, is a prime example of this flourishing type of norms-centered and empirically-grounded research conducted by legal scholars.⁸¹ One of the aims of this book is to contribute to, build on and carry forward the rich and growing body of socio-legal research and literature in this area.

It should also be noted that norms and values are central concepts not just in law and the social sciences but also in many other academic fields.⁸² These two concepts are thought of as being at the “crossroad of a large number of scientific disciplines”.⁸³ Indeed, much of human activity and behavior is determined or can be explained in relation to norms,⁸⁴ and values are considered “the main dependent variable in the study of culture, society, and personality, and the main independent variable in the study of social attitudes and behavior”.⁸⁵ Both serve as “guides and determinants” of individual’s and groups’ worldviews and behaviors.⁸⁶ Kluckhohn notes the relevance of these two concepts to inter- and multi-disciplinary research: “[t]he concept

⁷⁷ Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 159; Jack Gibbs, “The Sociology of Law and Normative Phenomena” 315; Jack Gibbs, *Norms, Deviance, and Social Control* 2.

⁷⁸ Jack Gibbs, “The Sociology of Law and Normative Phenomena” 315 and 322.

⁷⁹ Robert Ellickson, “The Evolution of Social Norms” 63; see also Robert Cooter, “Normative Failure Theory of Law” 949.

⁸⁰ Richard McAdams and Eric Rasmusen, “Norms and the Law” 1609.

⁸¹ See Robert Ellickson, *Order without Law*; Richard McAdams and Eric Rasmusen, “Norms and the Law” 1589 and 1609.

⁸² Jack Gibbs, “Norms: The Problem of Definition and Classification” 594; Milton Rokeach, *The Nature of Human Values* ix.

⁸³ Goran Therborn, “Back to Norms!” 863 and 879.

⁸⁴ Jack Gibbs, *Norms, Deviance, and Social Control* 2 and 16.

⁸⁵ Milton Rokeach, *The Nature of Human Values* ix and 3.

⁸⁶ Milton Rokeach, *The Nature of Human Values* 24.

of ‘value’ supplies a point of convergence for the various specialized social sciences, and is a key concept for the integration with studies in the humanities. Value is potentially a bridging concept which can link together many diverse specialized studies”.⁸⁷ The notion that social norms and “values affect the shape of technology” is well understood in the field of Science and Technology Studies (STS).⁸⁸ It is widely accepted, for instance, that “[c]omputer and information systems embody values”.⁸⁹ Thus, “[m]ore than any other concept”, norms and values hold the “promise of being able to unify apparently diverse interests of all the sciences concerned with human behavior”.⁹⁰ Therefore, focusing on norms and values is critical for conducting the interdisciplinary socio-techno-legal approach espoused in this book. It should be noted that the term norm is used as shorthand for social norm and these terms are synonymous and are used interchangeably in this book. Section 3.2 provides a further conceptual elaboration of norms and values.

1.5 Methodology

1.5.1 SOCIO-TECHNO-LEGAL STUDY

In order to examine the laws, technologies, norms and values that are pertinent to makers and hacktivists, this book adopts an interdisciplinary socio-techno-legal approach. A similar “socio-technical legal” approach has been put forward to deal with the problem of regulating cyberspace,⁹¹ but the emerging “socio-legal turn” in technology law scholarship can still be furthered by adopting a hybrid approach that combines technology law, socio-legal studies, and STS, which are

⁸⁷ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 389; Milton Rokeach, *The Nature of Human Values* 3.

⁸⁸ Helen Nissenbaum, “How Computer Systems Embody Values” 120 and 118; see also Trevor Pinch and Wiebe Bijker, “The Social Construction of Facts and Artefacts” 428; see also Sven Dietrich and others “Ethics in data sharing”.

⁸⁹ Helen Nissenbaum, “How Computer Systems Embody Values” 120 and 118.

⁹⁰ Milton Rokeach, *The Nature of Human Values* 3; see also Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 163.

⁹¹ Andrew Murray, *The Regulation of Cyberspace* 37.

interdisciplinary fields themselves. It may be said then that this book's conceptual and methodological approach is doubly interdisciplinary since these three fields require interdisciplinary research in their own right.

1.5.1.1 Socio-legal studies

The field of socio-legal studies has a broader orientation to the theories and methods that can be used for legal research. According to the Socio-Legal Studies Association's (SLSA) Statement of Principles of Ethical Research Practice, "Socio-legal studies embraces disciplines and subjects concerned with law as a social institution,⁹² with the social effects of law, legal processes, institutions and services and with the influence of social, political and economic factors on the law and legal institutions." Socio-legal study is interdisciplinary or multidisciplinary by nature and covers "a range of theoretical perspectives and a wide variety of empirical research and methodologies".⁹³ One of its main aims is to "produce socially-informed research about law".⁹⁴ In this book, I approach socio-legal studies as primarily legal research that is informed by social science theories and methodologies and grounded in empirical data.⁹⁵

This book adopts a socio-legal approach since this type of research normally entails conducting fieldwork about a particular social group located at a specific research site. Moore refers to this field site as a "semi-autonomous social field", which she describes as having the ability to "generate rules and customs and symbols internally, but that it is also vulnerable to rules and decisions and other forces emanating from the larger world by which it is surrounded".⁹⁶ According to Bour-

⁹² Socio-Legal Studies Association, "Statement of Principles of Ethical Research Practice".

⁹³ Socio-Legal Studies Association, "Statement of Principles of Ethical Research Practice"; Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* 1.

⁹⁴ Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* 2.

⁹⁵ See Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* 3.

⁹⁶ Sally Falk Moore, "Law and Social Change" 720.

dieu, “The social field can be described as a multi-dimensional space of positions such that every actual position can be defined in terms of a multi-dimensional system of coordinates whose values correspond to the values of the different pertinent variables”.⁹⁷ He further elaborates, “This field is neither a vague social background nor even a milieu” but “is a veritable social universe where, in accordance with its particular laws, there accumulates a particular form of capital where relations of force of a particular type are exerted. This universe is the place of entirely specific struggles”.⁹⁸ As a result, “a social field is the site of struggle, of competition for control”.⁹⁹ It should be noted though that while a social field “has rule-making capacities, and the means to induce or coerce compliance... it is simultaneously set in a larger social matrix”.¹⁰⁰ The concept of the semi-autonomous social field is exceedingly appropriate in examining the interactions between hacker norms and values and technology laws and policies since “[i]t draws attention to the connection between the internal workings of an observable social field and its points of articulation with a larger setting”.¹⁰¹ As such, this book considers various hacker sites like hackerspaces and hacker events as semi-autonomous social fields, which have their own internal norm-making capabilities that interact with external laws.

1.5.1.2 Science and technology studies

The “socio” and “techno” portions of the research are supported by STS. Technologies are not products created in a vacuum but are the result of various legal, socio-economic and cultural values and decisions.¹⁰² Informed by the “social constructivist view of technology” advocated in STS, which believes “science and technology are both socially constructed cultures and bring to bear whatever cultural resourc-

⁹⁷ Pierre Bourdieu, “The social space and the genesis of groups” 724.

⁹⁸ Pierre Bourdieu, *The Field of Cultural Production* 163-164.

⁹⁹ Richard Terdiman, “Translator’s Introduction” 808.

¹⁰⁰ Sally Falk Moore, “Law and Social Change” 720.

¹⁰¹ Sally Falk Moore, “Law and Social Change” 742.

¹⁰² Jonathan Zittrain, *The Future of the Internet* 20.

es are appropriate for the purposes at hand”,¹⁰³ this book affirms that technology is not neutral. It is a product of different contexts and social forces. This is an important point to bear in mind especially in the case of technological groups who sometimes claim that they are engaged in purely technical or scientific matters. A social constructivist view shows that this is never the case, and that through the process of technology making, technologists can and do shape society despite their protestations to the contrary. STS furthermore offers a wealth of literature on how technology and society mutually shape and co-produce each other.¹⁰⁴ Examining technologies from the perspective of STS is relevant to the aims of this book since technologies (e.g., the Arduino open-source, single-board microcontroller which is at the heart of many maker creations) embody and support norms and values and thus exert a profound influence on the actions of hackers and can also reveal the reasons and meanings behind hacking activities.

1.5.1.3 Technology law research

Technology law constitutes another core aspect of the socio-techno-legal approach applied in this book. By technology law, I mean the body of legislative enactments, administrative rules, judicial rulings, executive issuances, and acts of co-regulation or self-regulation that concern or relate to technologies and their creation, access and use. This research examines the technology laws and polices that specifically affect and are most relevant to hacking. Given that hacking is about the creative and innovative use of technology, the pertinent technology laws are those that concern or involve access to and use of information and technology. Computer crime laws are thus germane to hacking since these laws proscribe what people can or cannot lawfully do with computer data and systems. Doctrinal legal analysis is carried out on computer crime laws that are most relevant to makers and

¹⁰³ Trevor Pinch and Wiebe Bijker, “The Social Construction of Facts and Artefacts” 404.

¹⁰⁴ Sheila Jasanoff, “Ordering knowledge, ordering society” 15.

hacktivists in the Netherlands such as the Council of Europe's Convention of Cybercrime, the Cybercrime Directive and their national implementations.¹⁰⁵ The Convention on Cybercrime is particularly significant because it is the international instrument that is the legal foundation of many national computer crime laws around the world, including the Netherlands. The research also analyzes intellectual property laws since most (if not all) of the technologies, software and information that makers and hacktivists use and deal with are covered by intellectual property rights. The book focuses on international, regional and national intellectual property laws like the Berne Convention, the Copyright Directive, the Software Directive and their national implementations, especially in the Netherlands and across Europe.¹⁰⁶ Furthermore, legal research is conducted on contract and anti-circumvention laws because these laws can be used to modify or extend the legal effects and social impact of computer crime and intellectual property laws. For instance, certain rights granted to users like their ability to make personal and non-commercial copies of copyrighted works can be bargained away through contract and/or defeated with the use of digital rights management and other copy protection mechanism. The WIPO Internet Treaties, the Copyright Directive and their national implementations are the applicable laws in these areas.¹⁰⁷

As a piece of technology law research, it should be noted though that this book is not only concerned with the laws affecting makers and hacktivists, but it adopts an approach that focuses on the actors themselves, their norms and values, and their technologies. So, aside from doctrinal legal research,¹⁰⁸ empirical research on makers and

¹⁰⁵ Convention on Cybercrime <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>> accessed 26 July 2013; Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

¹⁰⁶ Berne Convention; Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (Copyright Directive); Directive 2009/24/EC on the legal protection of computer programs (Software Directive); Dutch Copyright Act.

¹⁰⁷ WIPO Copyright Treaty; WIPO Performances and Phonograms Treaty; Dutch Copyright Act.

¹⁰⁸ Ian Curry-Sumner and others, *Research Skills: Instruction for Lawyers*.

hacktivists was undertaken. While empirical data was collected mainly from makers and hackers in the Netherlands, the norms, values and technologies of hackers from different parts of the world were also examined.

This empirical and socially-oriented approach to law and technology research is significant since research methods that underpin socio-legal studies, namely conducting primary data collection about social groups located at specific research sites, are not often utilized by lawyers or in traditional legal research.¹⁰⁹ Moreover, concepts drawn from socio-legal studies and STS have not been applied in an integrated manner. By analyzing the responses and effects that non-state actors (makers and hackers) and their norms, values and technologies have on law and policy (and vice versa), this book shows, both theoretically and methodologically, the value of a social scientific and norm-based approach to technology law. This approach can produce more systematic and grounded research, as well as more practical recommendations for legal reform.

This book thus aims to expand the subjects and methods used in technology law research. With regard to subject matter, this book focuses on the laws of nation-states as well as the norms, values and technologies of non-state actors. Furthermore, it utilizes empirical methods such as interviews with key informants, participant observation, and qualitative content analysis. It is hoped that this book, by contributing to the understanding of the legal and normative impact of innovators and their technologies, and by advancing a more social and actor-oriented perspective to technology law, can help lead to new or improved approaches to the regulation and governance of hackers and hacking and possibly other technical actors and activities.

¹⁰⁹ Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* 18.

1.5.2 QUALITATIVE RESEARCH

Norms and values are indeed highly relevant to better understanding and interpreting the actions, attitudes and beliefs of makers and hacktivists in relation technology law and policy. Ascertaining what these norms and values are, where to observe or find them, and how they relate to law is therefore the principal preoccupation of this book. Despite certain difficulties and complexities in studying norms and values (e.g., problems with observability, measurement, interpretation, indeterminacy, quantification, reliability and validity),¹¹⁰ on balance, these issues can be overcome by resorting to a combination of methodological approaches and empirical sources.¹¹¹ Standard research methods such as “formal and informal interviews, recording of normal conversations, analysis of the oral and written lore of the group” can be utilized to gather data and analyze the norms and values within a social field.¹¹² As Spates argues, in order to study values and other elements of a culture or subculture, it is critical to investigate them “in situ using multiple observation techniques. This is dictated by the subjective nature of values and the different social settings in which they emerge. Single techniques – even grounded ones – cannot provide complete portraits”.¹¹³ Doing data collection or fieldwork in the social domains of makers and hacktivists (whether in physical places like hackerspaces or in virtual online communities) is vitally important since, in these spaces, one can closely observe the depth, nuance and complexity of their ways of life. As Fine points out,

Norms and behavioral expectations should not be separated from the meaning systems of individuals who enact them or from interaction that occurs in local spaces in which they are enacted. The performance of norms involves a complex construc-

¹¹⁰ Milton Rokeach, *The Nature of Human Values* 26-27; Michael Hechter, “Should Values Be Written Out of the Social Scientist’s Lexicon” 215, 217, 220, 221 and 223; Jack Gibbs, *Norms, Deviance, and Social Control* 11-17; Steven Hiflin and Jane Piliavin, “Values: Reviving a Dormant Concept” 360.

¹¹¹ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 395-396; see Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 175.

¹¹² Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 406.

¹¹³ James Spates, “The Sociology of Values” 44.

tion based on the framing of local context, negotiation of the interest of social actors, and the narrative depiction of behavioral rules.¹¹⁴

The existence, content, source and influence of norms and values can therefore be investigated through qualitative research that examine all three of the following: (1) actors' actions and behaviors, (2) their verbal and written statements, assertions and testimonies about appropriate conduct and of the desirable, and (3) how they prescribe and enforce sanctions and incentives to ensure conformity.¹¹⁵

Hackers' behaviors, their statements, and the positive or negative responses they have to certain conduct are consequently the three primary data sources that were used to examine their norms and values.¹¹⁶ Interviews, participant observation and secondary research are useful for gathering these types of data.¹¹⁷ A mixed methods approach using "participant observation, in-depth interviews... and document analysis" has similarly been used by social scientists to investigate the norms of subcultures.¹¹⁸ While some scholars suggest the use of formal surveys for studying values and norms (which can tend to elicit very structured and confined replies from respondents),¹¹⁹ the above three methods (especially interviews and participant observation) are more open-ended, descriptive, and based on people's lived experience, and thus better suited for examining the variety and subtlety of people's processes of meaning-making.¹²⁰ Through the triangulation of multiple data sets and methods,¹²¹ both explicit and implicit dimensions of norms and values can be observed and taken into account.¹²²

¹¹⁴ Gary Fine "Enacting Norms" 161.

¹¹⁵ Bruce Dohrenwend, "A Conceptual Analysis of Durkheim's Types" 469-470 and 472; Jack Gibbs, "Norms: The Problem of Definition and Classification" 590; Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 396 and 403 (approval or disapproval of conduct can be "shown by many kinds of expressive behavior, by deeds of support and assistance").

¹¹⁶ See Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 404-405.

¹¹⁷ See Alan Bryman, *Social Research Methods* 432, 470, 471 and 557; see Mike Crang and Ian Cook, *Doing Ethnographies* 35, 37 and 60; see K.D. Opp "Norms" 10715-10716; see James Spates, "The Sociology of Values" 39.

¹¹⁸ Gary Fine "Enacting Norms" 146; see also Michael Hechter and Karl-Dieter Opp, *Social Norms* xiii; see also Reza Banakar and Max Travers, "Ethnography and Law" 70.

¹¹⁹ K.D. Opp "Norms" 10716; Milton Rokeach, *The Nature of Human Values* 27 (who used a values survey); Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 405-406.

¹²⁰ Alan Bryman, *Social Research Methods* 470.

¹²¹ Robert Yin, *Case Study Research* 114-116.

¹²² See Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 408.

1.5.3 INDUCTIVE AND INTERPRETIVIST APPROACH

In light of Spates' criticism of the deficiencies of deductive approaches to studying human beings and social interactions (where there is a tendency to impose theories and preconceptions on data rather than making conclusions based on the collected data), my approach is on the whole inductive, and any conceptualization or analysis is based on empirical data and built from the ground up.¹²³ In support of an inductive methodology, Hechter states, "In principle, values can be measured either by asking people to describe their own values or by imputing their values from observed behavior".¹²⁴ Spates further claims that values can be studied "from the ground up'... by undertaking systematic observation of people's values and by constructing grounded hypotheses concerning how such values operate in concrete social settings".¹²⁵ Social scientists, particularly those in the field of STS, endorse an inductive and qualitative approach to research, and their methodologies "have tended to be qualitative rather than quantitative, thickly descriptive rather than thinly reductionist or model-dependent, deconstructive rather than paradigmatic, self-consciously, often ironically, narrative".¹²⁶

In addition to examining everyday practices, Kluckhohn puts forward "the relative merits of studying values in circumstances of crises and threats.... The observation and investigation of behavior in crisis situations is particularly rewarding".¹²⁷ To illustrate, Maker-Bot's decision to stop releasing all of its technologies and know-how as open source (see Section 2.3.2.3) is an actual controversy or crisis through and from which I was able to observe, draw upon and interro-

¹²³ James Spates, "The Sociology of Values" 30, 31, 35 and 43 (in contrast to the highly theoretical and deductive approach of functionalist theory); see John Flood, "Socio-Legal Ethnography" 46; Alan Bryman, *Social Research Methods* 24.

¹²⁴ Michael Hechter, "Should Values Be Written Out of the Social Scientist's Lexicon" 220.

¹²⁵ James Spates, "The Sociology of Values" 43.

¹²⁶ Sheila Jasanoff, "Beyond Epistemology" 411.

¹²⁷ Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 407-408; see also Trevor Pinch and Wiebe Bijker, "The Social Construction of Facts and Artefacts" 408 ("the effectiveness of focussing on technological controversies").

¹²⁸ See Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 405 (who states "Both individual and group crises... and conflict situations... throw values into relief").

gate makers about their norms and values.¹²⁸

As Gibbs states, a “way to identify the norms of a social unit, [is] to solicit responses... to ‘normative questions’ such as: Do you approve or disapprove of smoking marijuana?”¹²⁹ For example, one of the questions that I posed to the makers I met was whether they approved or disapproved of MakerBot’s choice to make their technologies closed and proprietary.

Norms and values, furthermore, have explicit or implicit dimensions. Examining implicit norms and values can be challenging since their existence and performance can only be indirectly observed through people’s overt actions and behaviors, including their imposition of sanctions for deviant conduct. In addition, the content of these norms and values have to be inferentially constructed (and thus open to multiple interpretations) by the research subjects themselves, the researcher and even third persons. As Kluckhohn states,

some of the deepest and most pervasive of personal and cultural values are only partially or occasionally verbalized and in some instances must be inferential constructs on the part of the observer to explain consistencies of behavior. An implicit value is, however, almost always potentially expressible in rational language by actor as well as by observer.¹³⁰

Some scholars view the subjectivity and context-dependence of norms and values as proof that these elements of culture cannot be reliably observed and accurately measured.¹³¹ They point out that “people may conceal their values for strategic purposes” or they “may not know what their values really are”.¹³² However, these concerns or impediments to investigating norms and values are not insurmountable and they can be sufficiently addressed, overcome and even turned into

¹²⁹ Jack Gibbs, *Norms, Deviance, and Social Control* 11.

¹³⁰ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 397.

¹³¹ Michael Hechter, “Should Values Be Written Out of the Social Scientist’s Lexicon” 215 and 220; K.D. Opp “Norms” 10715-10716.

¹³² Michael Hechter, “Should Values Be Written Out of the Social Scientist’s Lexicon” 221.

an advantage by adopting an interpretivist perspective and approach.

Interpretivism, as a theoretical paradigm and methodological approach, is composed of different theories and schools of thought, but it generally places an emphasis on “the meanings individual actors give to social interactions, and the use of symbols, such as language, in the creation of that meaning”.¹³³ Rather than seeing the subjectivity and multiplicity of meanings of human action as troublesome variables that need to be controlled for or rooted out, interpretivism embraces such complexity and diversity and uses them as the very materials from which to understand people’s actions and behaviors. Weber’s method of *verstehen* (or understanding) underpins the interpretivist approach.¹³⁴ *Verstehen* is an analytic procedure that seeks to understand an individual’s or group’s actions by examining the specific meanings, intentions and interpretations that the actors themselves ascribe to their actions within their particular social world or cultural contexts.¹³⁵ Interpretivism therefore requires delving into the “meaningful, understandable, or interpretable”.¹³⁶ It is concerned with the important processes of meaning-making and interpretation of human and social action.¹³⁷ As Walter explains,

From the interpretivist perspective, the human world is a world of meaning in which our actions take place on the basis of shared understandings. To understand society, we need to understand people’s motives and interpretations of the world. The meanings actors give to their circumstances are the explanation of what they do.¹³⁸

In response to the concern raised earlier about actors strategically concealing their norms and values or putting forward “invented”

¹³³ Maggie Walter, *Social Research Methods* 17.

¹³⁴ Max Weber, *The Theory of Social and Economic Organization* (trans AM Henderson and T Parsons) 87; Lisa Webley, “Qualitative Approaches to Empirical Legal Research” 4.

¹³⁵ Peter Munch, “Empirical Science and Max Weber’s *Verstehen de Soziologie*” 28, 29 and 31; Guy Oakes, “The *Verstehen* Thesis” 20.

¹³⁶ Guy Oakes, “The *Verstehen* Thesis” 21.

¹³⁷ Guy Oakes, “The *Verstehen* Thesis” 22; Max Travers, “Qualitative Interviewing Methods” 230

¹³⁸ Maggie Walter, *Social Research Methods* 17-18.

interpretations, it bears stressing that interpretations, whether by the actor, the researcher or other parties, do not occur in a vacuum. Interpretations are located and must be understood in relation to “established patterns of thought and behavior” or “according to usual modes of thought and feeling” within a particular social context or cultural situation.¹³⁹ While an actor may strategically feign a particular interpretation (which itself can serve as useful and revealing data), such interpretation is subject to further analysis, comparison and even criticism through the triangulation of various empirical and analytical methods and sources mentioned above. For example, a hackers’ claim during an interview that hackers value privacy will be analyzed together with other empirical data such as his behavior, other statements he made, and the statements and actions of other hackers. The requirements of empirical grounding and shared understandings help guard against a potential slide to or accusation of relativism.¹⁴⁰

In short, a qualitative, inductive and interpretivist approach is particularly well suited to the study of the technologies, norms and values of makers and hackers. Focusing on norms and values is highly relevant given that these two elements of culture have a significant and far-reaching impact on meaning-making since they pertain to people’s expectations and evaluations of the appropriate and the desirable. Qualitative methods, especially in-depth interviews and participant observation, are especially appropriate for investigating and gathering data about the interpretations and insider’s perspective of hackers.¹⁴¹

¹³⁹ Peter Munch, “Empirical Science and Max Weber’s *Verstehen de Soziologie*” 31.

¹⁴⁰ Max Travers, “Qualitative Interviewing Methods” 230.

¹⁴¹ Maggie Walter, *Social Research Methods* 230; Alan Bryman, *Social Research Methods* 399.

1.6 Research methods

1.6.1 DATA COLLECTION

In gathering data, I utilized a mixed approach that combined doctrinal legal research with various types of qualitative methods. I conducted: semi-structured interviews with makers and hacktivists in the Netherlands; participant observation at hackerspaces and hacker events in the Netherlands; qualitative content analysis of documents, texts and materials produced by or about hackers; doctrinal legal research on technology laws and policies relating to hacking; and secondary research on literature and materials about hackers. Table 1.1 gives an overview of the data sets, data sources and data collection techniques used in relation to specific research questions. For research sub-question 1, I conducted secondary research on literature and materials written about hacking and hacker culture. To study the practices, norms and values of hackers in sub-question 2, I interviewed and observed makers and hacktivists themselves. In order to verify and triangulate the information and responses that I received or observed from my

Table 1.1 Research Questions and Data Collection

Research Sub-Questions	Data Set	Data Source	Data Collection Technique
------------------------	----------	-------------	---------------------------

CHAPTER ONE

	Elements and practices of hacker culture and characteristics of different types of hackers	Documents and other materials produced by hackers	Secondary research
		Literature and other materials about hackers produced by non-hackers	Secondary research
2. Practices, technologies, norms and values of makers and hackers	Hackers' written and unwritten rules of behavior, their technical projects and social processes and activities, their statements about their norms and values; their attitudes toward and beliefs about law, authority, rights and freedoms	Makers and hackers, hacker spaces and hacker events in the Netherlands	Interviews, participant observation
		Documents and other materials produced by makers and hackers	Secondary research
		Literature and other materials about hackers produced by non-hackers	Secondary research
3. Hacking-related laws and responses of public authorities to hacking	International, regional and national laws, administrative rules, judicial rulings, executive issuances, acts of co-regulation, and state policies and actions concerning hackers and hacking	Legal databases, library collections, and government and institutional websites	Doctrinal legal research
		Newspaper articles, government reports, legal databases, government and institutional websites	Secondary research

4. Makers' and hackers' perceptions and responses to laws	Extent of hackers' knowledge and experience of hacking-related laws, their statements and actions in response to these laws	Makers and hackers, hackerspaces and hacker events in the Netherlands	Interviews, participant observation
		Documents and other materials produced by makers and hackers	Secondary research

respondents,¹⁴² I also conducted qualitative content analysis of documents produced by and about hackers.¹⁴³ With regard to hacking-related laws in sub-question 3, the unit of analysis was various international, regional and national technology laws and policies that specifically affect hacking. Since the data consisted of laws and regulations, the use of doctrinal legal research was appropriate. In relation to sub-question 4, to find out how hackers perceived and responded to laws, I examined makers' and hackers' attitudes towards and interactions with the law and public authorities. I also investigated cases in the Netherlands where hackers directly engaged with and sought to change technology laws and policies. Aside from soliciting the views and opinions of makers and hackers about these cases, I also conducted secondary research on relevant news articles, scholarly papers and other materials.

Interviews and participant observation were the main sources of the empirical data that was collected, particularly with regard to the norms and values of makers and hackers. Data collection and fieldwork were conducted in the Netherlands from October 2012 to April 2015. The Netherlands has a long-standing and vibrant hacker community and there are over a dozen active hackerspaces in the country.¹⁴⁴ Since 1989, an international hacker camp has been held in the

¹⁴² Robert Yin, *Case Study Research* 114-116.

¹⁴³ Alan Bryman, *Social Research Methods* 432

Netherlands every four years and is attended by thousands of hackers from around the world.¹⁴⁵ The interviewees and field sites were selected using non-probability sampling, specifically snowball sampling and purposive sampling.¹⁴⁶ Snowball sampling was quite useful because at the start I did not personally know Dutch makers and hacktivists. I was able to make initial contact and gain access to the Dutch hacker community by going to a popular, family-friendly technology fair held in a city in the Netherlands where technically minded people, including hackers and makers, showed off their creations and inventions to the general public. I was especially fortunate because, at the fair, an area was specifically allocated for hackerspaces where they could give training to the attendees (e.g., how to solder) and publicize their spaces and get new members. I was able to introduce myself to one group who invited me to attend a subsequent event. From this initial meeting, I was able to slowly expand and grow my network of contacts by asking gatekeepers and members of the hacker community to recommend other hackers that I should meet and places and events that I should go to.¹⁴⁷ To meet more potential interviewees and to conduct participant observation, I also visited places and attended events that makers and hacktivists go to or hang out such as hackerspaces, hacker camps and hackathons. As a complement to snowball sampling, I also used purposive sampling in selecting persons to interview.¹⁴⁸ In purposive sampling, the aim is “not to seek to sample research participants on a random basis” but “to sample cases/participants in a strategic way, so that those sampled are relevant to the research questions that are being posed”.¹⁴⁹ Interviewees were chosen based on the following non-cumulative criteria: (a) they were active members of a hackerspace or the hacker community; (b) they were engaged in hacking projects or

¹⁴⁴ See <http://hackerspaces.nl/> (accessed on 22 April 2014).

¹⁴⁵ Maxigas, “Hacklabs and hackerspaces” 5; Tatiana Bazzichelli, *Networking: The Net as Artwork* 143.

¹⁴⁶ Maggie Walter, *Social Research Methods* 111.

¹⁴⁷ See Mike Crang and Ian Cook, *Doing Ethnographies* 19-20.

¹⁴⁸ Alan Bryman, *Social Research Methods* 418.

¹⁴⁹ Alan Bryman, *Social Research Methods* 418; Maggie Walter, *Social Research Methods* 111.

activities that had legal implications or impact; (c) they were involved in or knowledgeable about cases where hackers challenged or sought to change technology laws and policies in the Netherlands; and/or (d) they had personal experience dealing with the law and public authorities because of their projects or activities.

With regard to interviews, each respondent was provided a copy of the participant information sheet, which explained: the purpose of the study, the benefits and disadvantages of participating, that their identities and personal information would be kept confidential, and what would happen to the collected data. During their respective interviews, respondents were requested to sign a consent form that confirmed, among other things, that: their participation was voluntary and they could withdraw at any time; the data they provided may appear in published research; they would not be named or identified in any publication; and they agreed to the recording of the interviews. The semi-structured interviews were conducted using an interview guide (Appendix A). The interview guide contained a list of general topics for discussion, but each interview was customized based on the respondent's specific background and depending on whether he or she was a maker, a hacktivist, or another type of hacker. Regardless of the differences among the respondents, all interviews concentrated on the following main discussion points: the meaning or purpose of hacking for them; the techno-social projects or campaigns they were involved in; the legal problems or difficulties they encountered; their knowledge or awareness of applicable laws; their attitudes or responses to laws and public authorities; and their views and opinions about cases where hackers came into conflict with law. A total of twenty-one interviews were conducted. Most were face-to-face interviews, three were done

through telephone or internet telephony, and one via email. The interview respondents consisted of twelve makers, six hacktivists, two ethical hackers, and one government official. The in-person and telephone interviews, which were approximately an hour long, were audio recorded and then transcribed. I also had many informal conversations with members of the hacker community at hackerspaces and other hacker events.

Empirical data was also collected through participant observation during fieldwork at various hacker events and sites. Participant observation “involves the researcher observing first hand in the research setting. The researcher is free to be an active participant in the normal routines of the research”.¹⁵⁰ As it was neither practical nor feasible to request all participants and attendees to sign consent forms in these situations, I informed the organizers or gatekeepers about my purpose and provided them with a participant information sheet. In one event, the organizers even announced my presence to the attendees so the latter would be made aware or informed of who I was and what I was doing, and they could approach me to ask questions. Getting the permission and support of gatekeepers was essential because, while most if not all of the hackers that I met were friendly and accommodating, they were averse to or wary of the police and other public authorities. Being connected to a university and the fact that I was doing academic research helped a lot in gaining access to the Dutch hacker community. In any event, in order to ensure the anonymity and confidences of the people that I observed or informally conversed with, I focused on the behaviors and statements of people in general or in aggregate rather than attributing such actions to specific individuals. Thus, people at these events would not be specifically identified or identifiable. If it so happened that a person needed to be singled out because his or her actions were especially significant or unique, I would have asked that

¹⁵⁰ Maggie Walter, *Social Research Methods* 82; see also Alan Bryman, *Social Research Methods* 714.

person to sign a formal consent form. But this was never the case.

While conducting participant observation, I collected data in a variety of ways and with different tools. I used a tablet or smartphone to quickly and inconspicuously jot down notes during events since these were less intrusive to use in hacker events where it is a common to see people using mobile phones, computers and other electronic gadgets. I also had a small pocket notebook where I could write down the names and contact information of new contacts and potential interviewees. In addition, I used a digital camera to take pictures of specific locations, settings and objects. Taking pictures during fieldwork was helpful because I could easily and quickly capture important, rich details (rather than having to draw everything on paper) and they acted as good memory aids. Unless people formally consented, I made sure to not include people in the pictures I took. I wrote down my observations and notes in a large notebook in the evening of or the morning after the event in order to capture and remember as much information as possible of what took place. In total, I undertook participant observation at thirteen places and events (i.e., six hackerspaces, two hacker camps, three hacking and technology-related conferences, one technology fair and one hackathon). My field notes from these events formed part of the empirical data and was analyzed as well.

1.6.2 CODING AND ANALYSIS

The collected data was analyzed using thematic analysis. Thematic analysis is “a form of qualitative analysis whereby the researcher seeks to identify themes that emerge from within the data”.¹⁵¹ A key part of thematic analysis is coding, which is the process “whereby data are broken down into component parts, which are given names”.¹⁵² Coding entails “naming segments of data with a label that simultane-

¹⁵¹ Maggie Walter, *Social Research Methods* 398.

¹⁵² Alan Bryman, *Social Research Methods* 568; see also Maggie Walter, *Social Research Methods* 324.

ously categorizes, summarizes, and accounts for each piece of data”.¹⁵³ A priori codes based on the research questions and analytical framework were initially used to code and analyze the data. These a priori codes are “determined prior to the data analysis” and “are either developed through an understanding of the literature, or that have already been deemed significant”.¹⁵⁴ As the analysis progressed however, inductive codes (“which emerge from the data being analysed”)¹⁵⁵ and in vivo codes (those derived “from the natural language of people in the social context being studied”)¹⁵⁶ were also reflexively developed and applied. Together, these a priori, inductive and in vivo codes comprised this research’s code list or coding system (Appendix B).¹⁵⁷ Specifically with regard to the interview data, it was transcribed, coded and analyzed using the qualitative data analysis software ATLAS.ti.¹⁵⁸ At the start of my research, for instance, I developed a working list of codes representing discrete categories of hacker norms and values.¹⁵⁹ The initial codes were constructed based on an extensive review and examination of the existing literature on hacker culture, and after conducting pilot interviews to test and verify the codes as well as the interview guide. Elements and portions of the codes were also publicly presented at hacker conferences to give members of the hacker community an opportunity to provide feedback and even contest the substance and formulation of the codes. It should be noted that Rokeach’s influential research on human values was similarly based on the creation of a “previously constructed list of terminal and instrumental values”.¹⁶⁰

In order to prevent the codes from predetermining the actual norms and values that I found and exerting too much influence on the interview respondents, I treated the list of codes as a working

¹⁵³ Kathy Charmaz, *Constructing Grounded Theory* 43; see also Susanne Frieze, *Qualitative Data Analysis with ATLAS.ti* 82.

¹⁵⁴ Maggie Walter, *Social Research Methods* 324-325.

¹⁵⁵ Maggie Walter, *Social Research Methods* 325.

¹⁵⁶ Alan Bryman, *Social Research Methods* 573; see also Susanne Frieze, *Qualitative Data Analysis with ATLAS.ti* 92.

¹⁵⁷ Maggie Walter, *Social Research Methods* 263; see also Alan Bryman, *Social Research Methods* 298-299.

¹⁵⁸ See Susanne Frieze, *Qualitative Data Analysis with ATLAS.ti*.

¹⁵⁹ See Maggie Walter, *Social Research Methods* 324-325.

¹⁶⁰ Milton Rokeach, *The Nature of Human Values* 27-29.

guide that had to be continuously updated or modified based on the data that was gathered. In this way, the codes served as an index (as opposed to a complete taxonomy) of the norms and values that I could rather than should observe. For example, during interviews, the codes were shown to respondents as a means to assist or stimulate discussions about what they consider appropriate and desirable, particularly in relation to the techno-social projects they were involved in. Interviewees were also encouraged to explain, critique and even disagree with the codes themselves and the norms and values they signify. During the data collection process, I was also constantly on the lookout or searching for other norms and values from the statements and actions of the makers and hacktivists that I spoke to or observed. For example, the value of “fun and play” was added to the codes after a number of respondents specifically stated that it was an important value. The codes were thus never fixed or exclusive, and were subject to constant evaluation and change based on the data collected. To further advance the inductive approach, the codes were not precisely defined. In this way, by making the codes broad and open-ended, they retained the flexibility and elasticity to accommodate the multiple meanings that they may elicit from or may be ascribed to them by different hackers. Nevertheless, it bears pointing out that the codes were not completely free from any theoretical or conceptual framing, and they should be understood within the framework of the liberal democratic tradition, which has an unmistakable influence on the worldviews and actions of all types of hackers.¹⁶¹ Drawing from the concepts and notions of liberal democracy is all the more useful given that the technology laws and policies that apply to hacking are founded on the very same theories and principles.

¹⁶¹ See Gabriella Coleman, “Hacker Politics and Publics” 514; see Gabriella Coleman, “Code is Speech” 428 and 437; see Christopher Kelly, “Geeks, Social Imaginaries, and Recursive Publics” 185; see John Dryzek, “Liberal Democracy and the Critical Alternative”; see Michael Dizon, “Free and Open Source Software Communities, Democracy and ICT Law and Policy” 139-140; see Argyro Karanasiou, “The changing face of protests in the digital age” 103.

It may be noticed that the codes listed in Table 1.2 are couched in terms of values rather than norms. It should be noted though that norms and values are closely related to each other. Given the interdependent and symbiotic relationship between the two (see Section 3.2.2), any observation of a value inherently and simultaneously involves the perception of its correlative norms, and vice versa. The very notion of norms “implies the existence of shared values”¹⁶² and values equally involve normative propositions.¹⁶³ As Gibbs points out, “Norms are based on cultural *values*”.¹⁶⁴ It was indeed very difficult in practice to completely separate norms and values from each other as they were flipsides of the same coin.

Table 1.2 Codes: Hacker values

Anonymity	Freedom of information
Community development	Fun and play
Consensus	Individual autonomy and liberty
Creativity and innovation	Openness
Curiosity	Personal growth
Decentralization and self-governance	Privacy
Efficiency	Security
Equality and meritocracy	Social development
Freedom of access	Transparency
Freedom of expression	

¹⁶² Jack Gibbs, “Norms: The Problem of Definition and Classification” 589.

¹⁶⁴ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 390.

¹⁶³ Jack Gibbs, “Norms: The Problem of Definition and Classification” 586.

1.7 Overview of chapters

To better understand the relations and interactions between hackers and the law and to improve the regulations that impact hacking, an in-depth analysis of the social, technological and legal domains that affect makers and hacktivists is essential. Chapter 2 describes makers and hacktivists by situating them within the broader hacker culture and against the backdrop of the varied histories and typologies of hacking. The similarities as well as differences between makers and hacktivists and other types of hackers are highlighted particularly with regard to the technologies they used, their goals and motivations, the places and spaces they inhabited, and how they were treated by the law and public authorities. In Chapter 3, the focus is on social norms and values and it begins with a further theoretical elaboration of these key concepts. The chapter discusses the prominent norms and values of makers and hacktivists based on an analysis of the collected empirical data. It also examines hacker manifestos as a source for understanding their social goals and rules of behavior. Chapter 4 examines the technology laws and policies that specifically affect hacking: computer crime, intellectual property, contract and anti-circumvention laws. The chapter analyzes these laws from the perspective of the norms and values of makers and hacktivists, discusses areas of conflict and congruence, and assesses whether such laws tend to restrict and/or support hacking. Chapter 5 delves into the perceptions and attitudes of makers and hacktivists toward law and public authorities. It explores hackers' different responses to law – from ignoring and avoiding the law to changing and resisting it, and to using or working within the legal system. The chapter includes detailed studies of high-profile cases in the Netherlands such as the hacking of the electronic voting machines and the Dutch national public transport card where hacker sought to change the law through hacking. Chapter 6 sets out and explains the normative implications of the research and legal recommendations to improve technology laws and policies that could be undertaken. The chapter proposes a change in the law's typical response to hack-

ing. Rather than attempting to restrict or prosecute hacking, it would be better for public authorities to support and reach out to hackers through more collaborative and participatory approaches like the adoption and implementation of responsible disclosure rules for security testing and open data policies and initiatives to encourage creative and innovative uses of information and technology. Chapter 7 closes the book with a brief reflection on the significance of hacking to technology law and policy and the importance and prospects of socio-techno-legal research.

CHAPTER TWO

Hacker culture

In order to properly understand makers and hacktivists, it is important to situate them first within and in relation to the broader hacker culture and history that they are a part of. As explained below, hacker culture has its own particular and distinctive characteristics and practices that makers and hacktivists equally embrace and perform. Furthermore, hacker culture is composed of different types of hackers. Being the most recent hacker types, makers and hacktivists have been influenced by and also draw from other types of hackers. It is essential then to learn more about the culture and contexts that makers and hacktivists belong to.

2.1 Histories and dimensions of hacking

As with any culture or subculture, hacker culture is constituted by manifold elements: norms and values, beliefs and ideologies, practices, rituals and ceremonies, language, symbols, technologies, status and roles, social organization, processes of meaning-making, and ways of life.¹ Hacker culture is further complicated by the fact that it is made up of different types of hackers, who come from varied backgrounds, belong to wide-ranging demographics, and possess traits that make them all distinct.² Because it is neither monolithic nor homogenous, hacker culture is very hard to pin down and its boundaries are difficult to precisely define. While it is not possible to speak of a pure hacker culture or an archetypical hacker group, as explained in Sec-

¹ See Gary Fine "Enacting Norms" 141; see Anthony Giddens, *Sociology* 1115.

² See Bruce Sterling, *The Hacker Crackdown* 50.

tions 1.2.1 and 1.4.1, there are certain core elements and characteristics that are held in common by these loosely joined individuals and groups who call themselves and each other hackers.³ As Taylor says, “The connotations of hacking have changed significantly over time, even though the essential elements of the activity have remained relatively constant”.⁴ Despite these obstacles, it remains possible to sketch out the broad outlines and discernable features of hacker culture.

This chapter does not intend nor aspire to provide a definitive account of hacker culture and history. It seeks, however, to construct a workable typology and narrative about different hacker types and periods in order to contextualize the emergence and development of makers and hacktivists.⁵ Makers and hacktivists are separate and distinct types of hackers but they draw from and are part of hacker culture because they share a host of similar practices, experiences and beliefs with the wider community of hackers, including the common acts of hacking discussed in the previous chapter. To understand makers and hacktivists, it is essential to locate them first within the ever-changing historical and techno-social contexts of the broader hacker culture, and compare them with other types of hackers.

It is generally accepted that hacking’s origins can be traced back to the computer scientists and programmers at the Massachusetts Institute of Technology (MIT) in the United States in the late 1950s.⁶ They were the first to use the terms “hacker” and “hack” to describe themselves and their activities.⁷ But how exactly hacker culture developed and evolved from these first computer hackers to the different hackers types that were dominant in the past and those that are salient today is subject of varying interpretations and explanations from

³ See Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 204.

⁴ Paul Taylor, “From hackers to hacktivists” 627.

⁵ See Sheila Jasanoff, “Beyond Epistemology” 411.

⁶ Steven Levy, *Hackers* x; Eric Raymond, “A Brief History of Hackerdom” 4; Bruce Sterling, *The Hacker Crackdown* 50; Douglas Thomas, *Hacker Culture* ix; OHM 2013, “Hack”.

⁷ Sam Williams, *Free As In Freedom* 175-176; Steven Levy, *Hackers* 10; Eric Raymond, “A Brief History of Hackerdom” 4.

hackers and those who write about them. For Alleyne, there are three hacker ideal types – open hackers, clandestine hackers, and hacktivists.⁸ Using an anthropological approach, Coleman and Golub classify hackers based on their ethical or moral practices:⁹ hackers who adhere to “crypto-freedom and the politics of technology”¹⁰ place strong emphasis on the value of security, privacy and secrecy; those who espouse the ideals of “free software and the politics of inversion”¹¹ tend to highlight the importance of freedom, openness, accessibility, sharing and creativity; and hackers who find affinity with “the underground and the politics of transgression”¹² are more concerned with matters relating to power, individual autonomy, evasion, subversion and defiance. From the perspective of computer crime law, hacking is said to have “four distinct focal periods”: “the discovery of computer abuse (1946-76)”;¹³ “the criminalization of deviant computer use (1977-87)”;¹⁴ “the demonization of hackers (1988-1992)”;¹⁵ and “the censorship period (1993-[2001])”.¹⁶ The most comprehensive classification so far has been Taylor’s seven hacker generations, which builds on Levy’s account of early hackers – “true” hackers (late 1950s and 1960s), hardware hackers (1970s) and game hackers (1980s)¹⁷ – and appends hackers/crackers (mid-1980s to present), microserfs (1980s to present), open source hackers (mid-1980s to present), and hacktivists (mid-1990s to present).¹⁸ The typology of hackers that I adopt (which closely resembles Taylor’s) is set out and explained in the next section.

⁸ Brian Alleyne, “We are all hackers now” 17.

⁹ E. Gabriella Coleman and Alex Golub, “Hacker Practice” 256.

¹⁰ E. Gabriella Coleman and Alex Golub, “Hacker Practice” 259.

¹¹ E. Gabriella Coleman and Alex Golub, “Hacker Practice” 261.

¹² E. Gabriella Coleman and Alex Golub, “Hacker Practice” 263 and 266.

¹³ Richard Hollinger, “Computer Crime” 76.

¹⁴ Richard Hollinger, “Computer Crime” 78.

¹⁵ Richard Hollinger, “Computer Crime” 78.

¹⁶ Richard Hollinger, “Computer Crime” 79.

¹⁷ Steven Levy, *Hackers* v-vi.

¹⁸ Paul Taylor, “From hackers to hacktivists” 628-629.

Despite the heterogeneous character of hacker culture and the plurality of possible representations of hacker types,¹⁹ it is possible to link and organize the diverse histories of various hacker types and periods in order to construct an overarching narrative about makers and hacktivists vis-à-vis hacker culture according to four dimensions: (1) what technology they hacked; (2) why they hacked; (3) where they hacked; and (4) how the law and authorities responded to them. These four dimensions relate to my research questions and the socio-techno-legal approach advanced by this book, which concerns itself with the study of the multifarious and interconnected aspects of law, technology and society in relation to makers and hacktivists. As presented in Section 1.5.1, this book's multidisciplinary approach combines the concepts and methods used in socio-legal studies, science and technology studies (STS), and technology law, which are interdisciplinary fields in themselves.

The first dimension concerns technology, which is the primary focus of STS.²⁰ While the disputes over whether technology determines society (technology determinism) or whether technology is shaped by society (social determinism or instrumentalism) continue to be argued among STS scholars,²¹ a useful workaround to this well-worn debate is to embrace the idea that technology is socially constructed as well as socially constructing. In this way, technology may be thought of as semi-socially constructed and constructing,²² since technology and society co-produced one another.²³ According to Flichy, “the technical object is not only a functional entity; it also conveys meanings. The object is not only material; it is also symbolic”.²⁴

¹⁹ See Andrew Chadwick, *Internet Politics* 130.

²⁰ Wiebe Bijker, Thomas Hughes and Trevor Pinch, *The Social Construction of Technological Systems* 10-11.

²¹ Langdon Winner, *Autonomous Technology* 74-75; Patrice Flichy, *Understanding Technological Innovation* 3 and 19.

²² Trevor Pinch and Wiebe Bijker, “The Social Construction of Facts and Artefacts” 401 and 404; Patrice Flichy, *Understanding Technological Innovation* 76 and 80; Sheila Jasanoff, “What Judges Should Know About the Sociology of Science” 347; Langdon Winner, *Autonomous Technology* 87-88.

²³ See Sheila Jasanoff, “Beyond Epistemology” 397; see Anthony Giddens, *The Constitution of Society* 16, 25 and 374; see Patrice Flichy, *Understanding Technological Innovation* 70.

²⁴ Patrice Flichy, *Understanding Technological Innovation* vii.

Conceiving technology and society as interacting and mutually shaping each other can help resolve the determinism debates in STS.²⁵ Applied to hacking, this implies that understanding hacker culture is inseparable from knowing their technologies. As Pinch and Bijker explain, the “sociocultural and political situation of a social group shapes its norms and values, which in turn influence the meaning given to [a technology]”.²⁶ The socially constructed and constructing character of technology is plainly evident in how hacker culture developed from the late 1950s to the present day. The capabilities and affordances offered by specific types and models of computers and other technical innovations that hackers created and used serve as important markers and catalysts of the progress of hacking – from mini-computers to personal computers (PCs) to 3D printers to software and services employed and produced across global computing and communications networks.²⁷

While the examination of technology can reveal a great deal about the history of hacking, there are other elements of hacker culture that can be productively explored and analyzed. With regard to the second dimension – the why of hacking, norms and values are key concepts in socio-legal studies that can help explain why hackers behave in a certain way, why they design and build technologies with specific features, and how they view and respond to law and authorities. The reasons and motivations behind hacking will be discussed extensively in Chapter 3 on hacker norms and values.

With regard to the third dimension – the where of hacking, hackers, as social actors, do not exist as disembodied entities in a vacuum but their practices, norms and values are performed within specific techno-social fields and are subject to influences from both

²⁵ See Patrice Flichy, *Understanding Technological Innovation* 18, 39 and 53; Michel Callon, “The Study of Technology as a Tool for Social Analysis” 98.

²⁶ Trevor Pinch and Wiebe Bijker, “The Social Construction of Facts and Artefacts” 428.

²⁷ Eric Raymond, “A Brief History of Hackerdom” 5; see Ian Hutchby, “Technologies, Texts and Affordances”.

within and outside these settings.²⁸ The computer laboratories, computer club meetings, online forums and communities, hacker events and hackerspaces that hackers frequent and inhabit are examples of a “semi-autonomous social field”, which is a useful concept in socio-legal study (see Section 1.5.1.1).²⁹ For instance, it is meaningful to analyze a hackerspace or a hacker camp as a semi-autonomous social field because in this setting hackers “collectively enact, make visible, and subsequently celebrate many elements of their quotidian technological lifeworld”.³⁰ The physical and virtual spaces that hackers inhabit and the places where they hack are empirically rich sites where the interactions between hacker technologies, norms and values and technology laws can be better and more intimately observed. It is interesting to note that both socio-legal studies and STS share an interest in studying individuals and groups within particular social fields, networks and sites.³¹ STS scholars are known for conducting research in scientific and research laboratories,³² and socio-legal researchers go on “fieldwork” to collect data.³³ Going out and immersing oneself in the relevant social field is essential to really get to know one’s research subjects.

In connection with the fourth dimension, the relations between hackers and law are touched upon briefly in the narrative below, in particular how the law and authorities viewed and responded to the activities of different hacker types. However, observing and understanding the interactions between hacking and law is the central research aim of this book and, thus, cannot be accomplished in this or any single chapter. The investigation and discussion of how hackers interact with

²⁸ See John Griffiths, “What is Legal Pluralism?” 34.

²⁹ Sally Falk Moore, “The Semi-Autonomous Social Field as an Appropriate Subject of Study”.

³⁰ Gabriella Coleman, “The Hacker Conference” 50.

³¹ Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research* 16; Christine Hine, *Virtual Ethnography* 8; Christine Hine, “How Can Qualitative Internet Researchers Define the Boundaries of Their Projects?” 4 and 7.

³² Patrice Flichy, *Understanding Technological Innovation* vi-vii; see Bruno Latour and Steve Woolgar, *LABORATORY LIFE: The Construction of Scientific Facts*; see Bruno Latour, “Give Me a Laboratory and I will Raise the World”.

³³ John Flood, “Socio-Legal Ethnography” 37.

technology laws will span the entirety of this book, with the core of the analysis being largely set out in Chapters 5 and 6.

2.2 A narrative typology of hackers

The typology of six types of hackers that I present in the succeeding sections (i.e., computer scientists, computer hobbyists, underground hackers, free and open source software (FOSS) developers, hacktivists, and makers) corresponds closely with Taylor's list of seven generations of hackers.³⁴ However, my classification does not match perfectly with Taylor's since my explication on various hacker types and periods is primarily aimed at making sense of and contextualizing makers and hacktivists as part of hacker culture. Rather than calling the original MIT hackers as "true" hackers, which has a negative implication on succeeding hacker generations, I refer to them as "computer scientists and programmers", which is what their roles and jobs were at MIT. The hardware hackers in the 1970s are better dubbed as "computer hobbyists" since they actually dealt with both computer hardware and software and the term hobbyist or enthusiast more fittingly depicts how they would describe themselves in relation to computers. Due to the great degree of contestation and controversy surrounding the hackers/crackers in the 1980s, I had difficulty in finding an appropriate label for them. I opted to go with the term "underground hackers" since it fairly captures how the law viewed them and their activities and how they perceived themselves. In contrast to Taylor, I do not consider underground hackers to be the same as crackers (i.e., persons who are only interested in breaking or breaking into systems to steal information or cause damage).³⁵ As explained below, underground hackers, unlike crackers, are not primarily interested in causing damage to computers and data. It is worth noting that among hackers, they would

³⁴ See Paul Taylor, "From hackers to hacktivists" 628-629.

³⁵ "Cracker", *The New Hacker's Dictionary*; see also Sam Williams, "Free As In Freedom" 178; see also Paul Taylor, "From hackers to hacktivists" 628; see also Reid Skibell, "Cybercrimes & Misdemeanors" 918.

also prefer to call people who engage in malicious or destructive activities as crackers rather than hackers.³⁶ The term cracker was coined by members of the hacker community in the 1980s as a “defense against journalistic misuse of hacker” to refer to computer criminals.³⁷ It should be noted though that the use of cracker has not caught on outside of the hacker community. Furthermore, game hackers do not appear in my narrative since they do not figure prominently, if at all, in relation to makers and hacktivists. I also do not discuss the so-called microserfs (i.e., hackers who have been co-opted or sold out to pursue commercial interests) as a separate type since most hackers regardless of their type have worked pursuant to commercial interests at one time or another, and hackers on the whole (with the possible exception of hacktivists) are not completely against or adverse to business.³⁸ In fact, computer scientists, computer hobbyists and FOSS developers have played a defining role in the development of the information and communications technology industry. I agree with Taylor that FOSS developers and hacktivists are distinct hacker types, but I have included makers as another type of hacker that gained prominence in the mid to late 2000s.³⁹

The ensuing narrative presents different images of hackers. The intent is not to present an idealized image of hackers, but to shed light on and to reveal who the different types of hackers are and what actually takes place within their social worlds. The following descriptions of the different hacker types and periods are generally presented in chronological order. Bear in mind though that my list of hacker types is neither intended to be exhaustive nor exclusive as there are many other types of hackers that exist (e.g., cypherpunks, black hat and white

³⁶ “Hacker”, The New Hacker’s Dictionary <http://www.outpost9.com/reference/jargon/jargon_23.html#TAG833> accessed 26 January 2016; Eric Raymond, “How to Become a Hacker” <<http://www.catb.org/~esr/faqs/hacker-howto.html>> accessed 26 January 2016.

³⁷ “Cracker”, The New Hacker’s Dictionary <http://www.outpost9.com/reference/jargon/jargon_18.html#SEC25> accessed 26 January 2016.

³⁸ See Paul Taylor, “From hackers to hacktivists” 629.

³⁹ See Chris Anderson, *Makers*; see *Hackerspaces - The Beginning*; see Mark Hatch, *The Maker Movement Manifesto*.

hat hackers, etc.).⁴⁰ As I mentioned earlier, I have specifically selected those types that are of particular relevance to contextualizing and explaining the emergence and development of hacktivists and makers, who are the main subjects of this book. It should also be emphasized that the precise boundaries between the different hacker types and their respective periods are blurred and there are countless overlaps and intersections among them.⁴¹ The fluidity of the memberships and categorizations among hacker types can be partly attributed to the fact that hackers often wear many hats and assume multiple (even contradictory) roles concurrently or at different times. Furthermore, it is worth pointing out that the specific labels that I use to name and distinguish the different hacker types (e.g., underground hackers) are meant to be descriptive categories of the individuals and groups who make up hacker culture. In truth, hackers, regardless of their designated type or period, usually refer to themselves or each other as simply “hackers”.⁴²

A number of the sources and materials on hacker history that I use are non-academic literature written by journalists and mainstream authors. The reliance on these types of sources is necessary given that scientific research on hackers only began in earnest in the early 1980s and, especially for early hacker generations, these remain the only extant materials.⁴³ Despite their limitations when compared to scientific research and literature, these popular books and articles about hacker culture remain rich and valuable documentary sources in their own right since they are based on actual interviews and face-to-face dealings of the authors with hackers.⁴⁴ Furthermore, scholars and hackers alike use, cite and rely heavily on these non-academic materials as key texts

⁴⁰ See Stevy Levy, *Crypto*; see Paul Taylor, *Hackers* 23; see David Wall, *Cybercrime* 54; see Cassandra Kirsch, “The Grey Hat Hacker” 386 and 388.

⁴¹ Paul Taylor, *Hackers* x.

⁴² See Bruce Sterling, *The Hacker Crackdown* 59; see “Hacker”, *The New Hacker’s Dictionary*; see Steven Levy, *Hackers* 456.

⁴³ See Sherry Turkle, “The Subjective Computer: A Study in the Psychology of Personal Computation”.

⁴⁴ See Alan Bryman, *Social Research Methods* 543 and 554-555; see Steven Levy, *Hackers* 486-486; see Bruce Sterling, *The Hacker Crackdown* 10 and 250; see Robert Cringely, *Accidental Empires* x.

about hacker history and culture.⁴⁵ In any event, I have sought to verify the truth and accuracy of these non-scholarly sources by comparing them with each other to ferret out consistencies and divergences and analyzing them in light of available scientific research. Thus, as much as possible, factual statements within the narrative are supported by more than one source. Accounts and stories about hackers have tended to lie at the extremes of either being too negative or too positive about hacking. I have endeavored to present a reasonably fair and balanced picture of hackers by using a diverse range of sources and materials including those that do not paint hackers in a favorable light.

Authors who have extensively dealt with and written about hacker culture are often accused of being too friendly or partial to hackers and seeing them through rose-tinted glasses. The general empathy shown towards hackers and hacking by writers, journalists and researchers who have immersed themselves in hacker culture, myself included, does not stem from any preexisting bias or predisposition, but is the outcome of the authors' open, honest and fair communications and interactions with hackers.⁴⁶ As is often the case with these intersubjective encounters, researchers and writers who have dived deeply into and interacted intimately with a particular social field or community come away with a deeper understanding of and respect for (but not necessarily personal agreement with) the people they have studied and the culture they have observed.⁴⁷ This is distinguishable from and does not have to lead to the problem of "going native" or becoming an active supporter of the subjects' causes.⁴⁸ Greater understanding, sensitivity and empathy of the observer for his or her subjects can be expected when one sees the world through their eyes, but this does

⁴⁵ See Helen Nissenbaum, "Hackers and the contested ontology of cyberspace" 3-4; see Paul Taylor, "From hackers to hacktivists" 5-6; see E. Gabriella Coleman and Alex Golub, "Hacker Practice" 256-257; see Chaos Computer Club, "Hacker Ethics" <www.ccc.de/hackerethics> accessed 17 July 2013; see Paul Taylor, Hackers xi.

⁴⁶ Mike Crang and Ian Cook, *Doing Ethnographies* 13 and 46.

⁴⁷ See Mike Crang and Ian Cook, *Doing Ethnographies* 14-15 and 43.

⁴⁸ Alan Bryman, *Social Research Methods* 445.

not necessarily mean approval of their worldview.⁴⁹ For instance, while I observed a strong attitude of distrust for public authorities among the makers and hacktivists I met, at the end of this book, I still recommend the importance of hackers collaborating and working together with public authorities to improve technology laws and policies.

2.2.1 OF MINICOMPUTERS AND LABORATORIES – COMPUTER SCIENTISTS AND PROGRAMMERS

2.2.1.1 The Hulking Giants

Based on Levy's journalistic account of the early history of hacking, the introduction and use in the late 1950s and 1960s of computers such as the TX-0 and the PDP-1 and their successors was vital to the genesis of hacker culture.⁵⁰ It is noteworthy that the birth and growth of hacking corresponded with greater freedom and access to increasingly more advanced, interactive and "hackable" computers.⁵¹ Before the availability of these hacker-friendly machines, anyone interested in computing had to use large mainframe computers like the IBM 704, which hackers ominously and derisively called "the Hulking Giant".⁵² Access to and use of these expensive mainframe computers were limited and complicated due to technical and social factors. These mainframe computers were located in highly controlled and well-protected laboratories that were administered and guarded by authorized computer operators, whom early hackers likened to a kind of priesthood.⁵³ As Levy explains, "The IBM 704 cost several million dollars, took up an entire room, needed constant attention from a cadre of professional machine operators, and required special air conditioning".⁵⁴ People outside of the priesthood could not directly use or

⁴⁹ Alan Bryman, *Social Research Methods* 399; Mike Crang and Ian Cook, *Doing Ethnographies* 47.

⁵⁰ Eric Raymond, *The Cathedral and the Bazaar* 4.

⁵¹ See Steven Levy, *Hackers* 41.

⁵² Steven Levy, *Hackers* 5.

⁵³ Steven Levy, *Hackers* 5; Bruce Sterling, *The Hacker Crackdown* 60.

⁵⁴ Steven Levy, *Hackers* 5.

program these mainframe computers (much less study or modify the hardware and software) as only the anointed computer operators had direct access to and could feed programs (as batch-processed punch cards) into the Hulking Giants.⁵⁵ It is therefore not surprising that hacker culture emerged and blossomed with the availability of more accessible and modifiable technologies.

2.2.1.2 The TX-0

The TX-0 (pronounced “Tix Oh” and short for “Transistorized eXperimental computer zero”) was an experimental computer that used transistors rather than vacuum tubes, which made it smaller and easier to operate and maintain compared to the giant mainframe computers.⁵⁶ It had important technical innovations that made it more amenable to hacking: first, it had an actual computer monitor that made programming more interactive and immediate; second, programs could be fed into it using paper tapes that could be more conveniently produced using a typewriter-like Flexowriter rather than laborious punch cards; and, third, it was set up so that users could actually sit in front of the computer while programming and debugging their programs.⁵⁷ Levy explains the significance of these technical improvements of the TX-0 to the early hackers who were computer scientists and programmers in academic and research institutions in the late 1950s and the 1960s: “The user would first punch in a program onto a long, thin paper tape with a Flexowriter (there were a few extra Flexowriters in an adjoining room), then sit at the console, feed in the program by running the tape through a reader, and be able to sit there while the program ran”.⁵⁸

⁵⁵ Steven Levy, *Hackers* 5; Eric Raymond, “A Brief History of Hackerdom” 4; Pekka Himanen, “A Brief History of Computer Hackerism” 186.

⁵⁶ “TX-0 Computer, MIT Lincoln Laboratory, 1953-1957”; “TX-0 Computer”.

⁵⁷ “MIT TX-0 Computer 1953”; “TX-0 Computer, MIT Lincoln Laboratory, 1953-1957”; see Steven Levy, *Hackers* 14-16.

⁵⁸ Steven Levy, *Hackers* 15; see also Pekka Himanen, “A Brief History of Computer Hackerism” 186.

The social conditions surrounding the TX-0 also favored hacking. The early hackers, who were initially students and then became computer researchers at MIT, were invited to use the TX-0 by one of their former colleagues, and the technician in charge generally tolerated their use of the computer during off hours. While they had access to the computer during regular office hours,⁵⁹ computer hackers preferred to work at night and during the early hours of the morning when they had the computer all to themselves and they did not have to share computing time and power with other scientists at MIT's Research Laboratory of Electronics (RLE).⁶⁰

With the TX-0, there were no priests or intermediaries that controlled or prevented access. While the TX-0 was located in the RLE, the early hackers treated it more as a place to hangout and create rather than a formal laboratory.⁶¹ Instead of being suppressed or considered a cause for alarm by the university authorities and the US government (which provided major funding for early computer research), hacking was generally seen as a productive activity that should be encouraged or at least tolerated.⁶² According to Raymond, government agencies “deliberately turned a blind eye to all the technically ‘unauthorized’ activity; [they] understood that the extra overhead was a small price to pay for attracting an entire generation of bright young people into the computing field”.⁶³ As Sterling explains,

Most of the basic techniques of computer intrusion: password cracking, trapdoors, backdoors, trojan horses – were created in college environments in the 1960s.... Outside of the tiny cult of computer enthusiasts, few people thought much about the implications of “breaking into” computers. This sort of activity had not yet been publicized, much less criminalized.⁶⁴

⁵⁹ Steven Levy, *Hackers* 15-16 and 23.

⁶⁰ Steven Levy, *Hackers* 15-16 and 23.

⁶¹ Steven Levy, *Hackers* 15-16 and 30.

⁶² Steven Levy, *Hackers* 90, 98, 115; Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 198.

⁶³ Eric Raymond, “A Brief History of Hackerdom” 7.

⁶⁴ Bruce Sterling, *The Hacker Crackdown* 60.

The authorities' non-interference or support for early hacking activities could be explained by the fact that computer scientists were a relatively small and identifiable group, there were not many computers at the time and they were all located in either university, research, military or corporate settings, and the impact or sphere of influence of these early hacking activities (including any actual or potential damage or harm) could only be felt within the four walls of the computer laboratory and were thus not a cause for concern or alarm.⁶⁵

2.2.1.3 The PDP-1

With the subsequent introduction and use of the PDP-1 (or “Programmed Data Processor-1”), hacker culture truly flourished at MIT.⁶⁶ The PDP-1, which was created by Digital Equipment Corporation (DEC), was the first minicomputer and, like the TX-0 that inspired it, espoused the idea of “interactive computing”.⁶⁷ The PDP-1 had features that made it ideal for hacking: like the TX-0, the user could sit in front of the computer while programming; it was possible to attach different input and output (I/O) devices to it; and “it was the first commercial computer that focused on interaction with the user rather than the efficient use of computer cycles”.⁶⁸ In addition to these technical advantages, the PDP-1 and the space where it was housed became the center of the hacker community at MIT because the early computer hackers had free access to them in both physical and technical senses. The PDP-1 was set up in a room in the RLE that hackers designated as the Kluge Room.⁶⁹ It was a place where hackers could devote all of their time programming and working on the computer without much interference from gatekeepers and outsiders.⁷⁰ With the PDP-1 and its

⁶⁵ See Bruce Sterling, *The Hacker Crackdown* 60; Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 579; E. Gabriella Coleman, *Coding Freedom* 64-64.

⁶⁶ Steven Levy, *Hackers* 41; Eric Raymond, “A Brief History of Hackerdom” 4; “PDP-1 Restoration Project”.

⁶⁷ Larry Press, “Before the Altair” 28; Eric Raymond, “A Brief History of Hackerdom” 4.

⁶⁸ “PDP-1 Restoration Project”, Computer History Museum; see also George Michael, “The PDP-1”

⁶⁹ Steven Levy, *Hackers* 43.

⁷⁰ Steven Levy, *Hackers* 43.

successors, they had relatively unimpeded access to explore and learn about how the computer worked and close to full freedom to change and improve the computer's hardware and software. The ability and freedom to hack the PDP-1 produced important advances in computer science and engineering such as "early debugging, text editing, music and game programs, including the first computer video game, Spacewar".⁷¹ They were able to produce these innovations through hacking; they learned about the inner workings of a computer and how, by giving it the right instructions, they could create programs that made it perform various tasks; they had no qualms about breaking passwords, locks and other security devices in order to explore and gain access to computers and information; and they freely shared programs with each other by placing them in unlocked drawers. The early hackers were not concerned with keeping things secure since they saw this as a hindrance to the free access to and open use of knowledge and technology.

Even when the centers of hacking expanded, moved, and proliferated to other areas at MIT (such as the hacker utopia on the ninth floor of Tech Square) and to more cities and research laboratories, the interactive and hackable computers remained the centerpiece of the creative, innovative, and often chaotic spaces that hackers built around them.⁷² Turkle writes, "Hackers don't live only with computers; they live in a culture that grows up around computers".⁷³ In fact, it can be argued that the computers themselves served as spaces within which hacking took place. As über-hacker Bill Gosper recounted to Levy, "In some sense, we lived inside the damn machine. It was part of our environment. There was a society in there".⁷⁴ For the early hackers, com-

⁷¹ "PDP-1 Restoration Project", Computer History Museum; see also Pekka Himanen, "A Brief History of Computer Hackerism" 186.

⁷² Steven Levy, *Hackers* 65, 122, 123 and 133; Eric Raymond, "A Brief History of Hackerdom" 5; Stewart Brand, "SPACEWAR: Fanatic Life and Symbolic Death Among the Computer Bums" *Rolling Stone* (7 December 1972).

⁷³ Sherry Turkle, *The Second Self* 196; but see Paul Taylor, "From hackers to hacktivists" 631-632 (who discusses the negative effects of the early hackers' total immersion into computers).

⁷⁴ Steven Levy, *Hackers* 78; see also Sherry Turkle, *The Second Self* 191 and 204.

puters were simultaneously tools and spaces for making technology and changing their lives, and they were unconcerned about the authorities and the latter generally gave them free reign to do as they pleased.

2.2.2 OF MICROCOMPUTERS, GARAGES AND COMPUTER CLUBS – COMPUTER HOBBYISTS

2.2.2.1 The Altair

If the TX-0 and the PDP-1 and their successors were the computers that epitomize the original computer hackers, it was the MITS Altair 8800 (Altair) and the Apple II that defined the computer hobbyists in the 1970s. From a technical standpoint, the Altair was not in the same league as the minicomputers that were used by the original hackers, which were at the time very advanced, powerful and expensive computing machines. Built by the company Micro Instrumentation and Telemetry Systems (MITS) in Albuquerque, New Mexico, and launched in the January 1975 issue of *Popular Electronics*, a magazine for electronics enthusiasts, the Altair was a barebones digital, programmable computer.⁷⁵ Aesthetically speaking, it was a squat, blue and gray metal box with red lights and silver switches on its black face. Inside, it had five basic subsystems: a central processing unit (CPU) which “performs all the calculations, generates system timing, and makes all decisions”;⁷⁶ the memory for storing information in the form of bits (binary 1s and 0s);⁷⁷ a front panel that contained switches and LED status indicators that served as the computer’s main input and output interface;⁷⁸ a power supply;⁷⁹ and room for peripheral and memory expansion.⁸⁰ Compared to modern PCs, out of the box the Altair did not come with now standard I/O devices such as a keyboard, mouse

⁷⁵ Robert Cringely, *Accidental Empires* 61.

⁷⁶ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 34.

⁷⁷ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 36.

⁷⁸ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 37.

⁷⁹ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 38.

⁸⁰ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 38.

or display (users could subsequently add some of these peripherals).⁸¹ With regard to its operation, the Altair was not a paragon of interactive computing since instructions and programs had to be entered using its front switches and the results could only be displayed to the user in binary format.⁸² Levy describes the Altair's lack of user-friendliness: it was

... a box of blinking lights with only 256 bytes of memory. You could put in a program only by flicking octal numbers into the computer by those tiny, finger-shredding switches, and you could see the answer to your problem only by interpreting the flickety-flock of the LED lights, which were also laid out in octal.

Despite these limitations, the Altair had certain features and “affordances” that made it spark the computer revolution.⁸³ The fact that the Altair was not sold fully assembled but as a kit that users had to build themselves was not a shortcoming but a key feature. Having to put together the Altair themselves meant that computer hobbyists would not only be getting their own computers but they would also learn how computers worked. As Levy explains, “It was an education in itself, a course of digital logic and soldering skills and innovation”.⁸⁴ Price was also a factor.⁸⁵ In contrast to the minicomputers and main-frame computers that cost hundreds of thousands, if not millions, of dollars, the Altair was available to the general public for under US\$400.⁸⁶ At this price point, it was reasonably affordable, and a broader segment of society and not only well-funded researchers and laboratories could gain access to computing.⁸⁷ One reason why the Altair was relatively inexpensive was because it was made using off-the-shelf components and parts.⁸⁸ The use of off-the-shelf technologies

⁸¹ Robert Cringely, *Accidental Empires* 53.

⁸² Robert Cringely, *Accidental Empires* 53.

⁸³ See Tim Jordan *Hacking* 136; see Ian Hutchby, “Technologies, Texts and Affordances”.

⁸⁴ Steven Levy, *Hackers* 195.

⁸⁵ Steven Levy, *Hackers* 196.

⁸⁶ H. Edward Roberts and William Yates, “Altair 8800 Minicomputer, Part I” 34.

⁸⁷ See John Markoff, *What the Dormouse Said* 277.

⁸⁸ Steven Levy, *Hackers* 188.

meant that: parts were often readily available, commoditized and standardized; there was a greater likelihood that the components would be interchangeable and interoperable with those made by a wide range of other manufacturers; and, anyone (including other companies) could use the same or similar parts to build their own computers and peripherals.⁸⁹ The Altair's size and componentized design also made it possible to ship parts to hobbyists around the country for assembly in their own homes and garages, and, unlike the Hulking Giants, it could be built and used on a desk or work table, and it was portable enough to be brought and shown off at computer club meetings.⁹⁰

Of course, what made the Altair truly remarkable was that it was open and hackable in many respects. Designed as a "general-purpose computer",⁹¹ it did not have a fixed purpose but it could be made to perform a multitude of functions and uses by simply running different software or incorporating other hardware and peripherals to it. The Altair was built to run "thousands of possible applications" and infinitely expandable with "almost unlimited peripheral and memory expansion".⁹² Some potential uses that were envisioned for the Altair included being a programmable scientific calculator, an intruder alarm system, a digital signal generator, a brain for a robot, an automatic drafting machine, a signal analyzer, and a host of other devices.⁹³ As an electronics kit aimed at hobbyists, the Altair was so open that users could even request the company MITS to mail them the full assembly details (including etching and drilling guides, component-placement diagrams, and other information).⁹⁴

⁸⁹ See Nathan Rosenberg, "Technological Change in the Machine Tool Industry"; Steven Levy, *Hackers* 207.

⁹⁰ See H. Edward Roberts and William Yates, "Altair 8800 Minicomputer, Part I" 34; see Steven Levy, *Hackers* 201.

⁹¹ H. Edward Roberts and William Yates, "Altair 8800 Minicomputer, Part I" 34 and 38; see also Cory Doctorow, "Lockdown: The coming war on general-purpose computing".

⁹² H. Edward Roberts and William Yates, "Altair 8800 Minicomputer, Part I" 38.

⁹³ H. Edward Roberts and William Yates, "Altair 8800 Minicomputer, Part I" 38.

⁹⁴ H. Edward Roberts and William Yates, "Altair 8800 Minicomputer, Part I" 38.

2.2.2.2 The Homebrew Computer Club

The hackable or “generative”⁹⁵ nature of the Altair was not confined to its technical aspects but it extended to the many techno-social fields that it engendered and fostered. The Altair is credited for spurring the formation of “personal computer conferences, clubs, stores, users’ groups, software exchanges and company newsletters”.⁹⁶ These social events, activities and gatherings that centered on computers were meant to encourage technical innovation, knowledge sharing and community building. Software exchanges, for instance, were events announced in computer magazines where hobbyists came together to meet other kindred spirits and share programs that they or other people had written.⁹⁷ Like the original MIT hackers, the free sharing of information, technical know-how and programs was part of the culture of computer hobbyists.⁹⁸

Cooperation and sharing were the main thrusts of the most well-known computer club in the 1970s – the Bay Area Amateur Computer Users Group (better known as the Homebrew Computer Club).⁹⁹ Fred Moore, an activist, and Gordon French, an engineer, conceived the Homebrew Computer Club as a venue where people interested in computers could come together to teach and learn from each other.¹⁰⁰ As the flyer calling for the first meeting stated, the Homebrew Computer Club was “... a gathering of people with like-minded interests. Exchange information, swap ideas, help work on a project, whatever...”.¹⁰¹ It is interesting to note that the first meeting of the club on Wednesday, 5 March 1975, was held in a garage and the main item on the agenda was a working Altair that was on loan from MITS to the People’s Computer Company, an organization that

⁹⁵ See Jonathan Zittrain, *The Future of the Internet* 2-3.

⁹⁶ Forrest Mims III, “The Tenth Anniversary of the Altair 8800” 60.

⁹⁷ See Christina Lindsay, “From the Shadows” 38.

⁹⁸ Steven Levy, *Hackers* 118 and 232 (who called them “hardware hackers”); Pekka Himanen, “A Brief History of Computer Hackerism” 187.

⁹⁹ Steven Levy, *Hackers* 202-203; see Pekka Himanen, “A Brief History of Computer Hackerism” 187.

¹⁰⁰ Steven Levy, *Hackers* 197-199.

¹⁰¹ John Markoff, *What the Dormouse Said* 275-276; see also Steven Levy, *Hackers* 199.

introduced children to computing and programming and hosted weekly Wednesday evening potlucks for computer aficionados.¹⁰² Pursuant to an egalitarian, anti-establishment and countercultural ethos, the Homebrew Computer Club “had no membership requirements, asked no minimum dues..., and had no election of officers”.¹⁰³ Its fortnightly meetings were subsequently held in various places including high-tech hubs like the Stanford Artificial Intelligence Lab (SAIL) and the auditorium of the Stanford Linear Accelerator (SLAC).

Hobbyist gatherings and garages were the main spaces and sites where hacking in the truest sense of the word took place: they explored and learned about computers by designing and creating one themselves; they had no qualms about breaking or being in breach of someone’s copyright if this meant getting access to important knowledge and technology and sharing it with others; but, like the early MIT hackers, they were more concerned with making computers free and open rather than keeping them secure.¹⁰⁴ During club meetings, members would have a chance to tell the whole group what they were working on, people could also socialize and speak with others individually, and there were scheduled talks, demonstrations and new product announcements.¹⁰⁵ They were not fond of secrecy and they openly disclosed rumors and secrets about new technological developments (including a chip containing Atari’s soon to be launched videogame Pong).¹⁰⁶ They unstintingly gave away tips and advice to others, and showed off the computers, boards and devices that they created in their homes and garages.¹⁰⁷ Part of the dynamic in these gatherings was the notion of building on the work of others and sharing it back with the community.¹⁰⁸ The social norm was that everyone helped

¹⁰² Steven Levy, *Hackers* 165, 171 and 201; John Markoff, *What the Dormouse Said* 266; Larry Press, “Before the Altair” 29.

¹⁰³ Steven Levy, *Hackers* 203; see also John Markoff, *What the Dormouse Said* xiii and xv; see also Pekka Himanen, “A Brief History of Computer Hackerism” 188; see also Bruce Sterling, *The Hacker Crackdown* 57.

¹⁰⁴ See Robert Pool, “A History of the Personal Computer” 94.

¹⁰⁵ Steven Levy, *Hackers* 216; John Markoff, *What the Dormouse Said* 277.

¹⁰⁶ Steven Levy, *Hackers* 218-219.

¹⁰⁷ Steven Levy, *Hackers* 212, 214 and 216.

¹⁰⁸ Steven Levy, *Hackers* 219 and 220.

each other for free.¹⁰⁹ According to Levy, some members “used the club as a source of ideas and early orders, and for the beta-testing of prototypes. Whenever a product was done you would bring it to the club and get the most expert criticism available”.¹¹⁰ Like MITS’s approach to the Altair, hobbyists were likewise expected to “distribute the technical specifications and the schematics [of their creations] – if it involved software, you would disclose the source. Everyone could learn from it, and improve on it if they care to and were good enough”.¹¹¹

The free and open exchange of information was truly at the heart of these gatherings; computer hobbyists believed that “[l]ike the unfettered flow of bits in an elegantly designed computer, information should pass freely among the participants in Homebrew”.¹¹² For the Homebrew Computer Club, “the free sharing of information was not just an aspect of it but the essential reason for its existence”.¹¹³ It may be said that the great fascination with early microcomputers is rooted in the fact that hobbyists perceived the general-purpose computer as being both the manifestation of and the means to achieve their egalitarian, democratic and countercultural ideals and aspirations of the late 1960s and early 1970s.¹¹⁴ It was both a tool and a product of hacking. Levy explains the philosophy of computer hobbyists:

They were hackers. They were curious about systems as the MIT hackers were, but, lacking daily access to the PDP-6s, they had to build their own systems. What would come out of these systems was not as important as the act of understanding, exploring, and changing the systems themselves – the act of creation, the benevolent exercise of power in the logical, unambiguous world of computers, where truth, openness, and democracy existed in a form purer than one could find anywhere else.¹¹⁵

¹⁰⁹ Steven Levy, *Hackers* 220.

¹¹⁰ Steven Levy, *Hackers* 221.

¹¹¹ Steven Levy, *Hackers* 221.

¹¹² Steven Levy, *Hackers* 214 and 216; see also John Markoff, *What the Dormouse Said* xx.

¹¹³ John Markoff, *What the Dormouse Said* 282.

¹¹⁴ John Markoff, *What the Dormouse Said: How the 60s Counterculture Shaped the Personal Computer Industry* xii.

¹¹⁵ Steven Levy, *Hackers* 191

2.2.2.3 The Apple II

In hindsight, it seems inevitable that the “most important computer in history” would have its genesis in the Homebrew Computer Club’s open, innovative and collaborative milieu.¹¹⁶ The Apple II, which was launched at the First Annual West Coast Computer Faire in 1977, is considered the first commercially successful, mass-market microcomputer.¹¹⁷ Part of its success may be attributed to the fact that it was a low-cost consumer product aimed at ordinary users rather than a kit targeted to hobbyists.¹¹⁸ The Apple II had a number of features and innovations that made it a world-changing product. First, it came in a simple yet sleek beige plastic case that had a built-in keyboard so it resembled a typewriter.¹¹⁹ There was clearly an attempt to make it look and feel like a consumer device that had a place in everyone’s home or office.¹²⁰ Second, a television or monitor could be conveniently placed on top of the case and attached to serve as the display.¹²¹ The Apple II could show texts and graphics on the screen in different resolutions and in color.¹²² Third, the computer language BASIC was built into the computer’s read-only memory (ROM), which meant that users could start up the Apple II and work right away and create programs without having to install or run additional software.¹²³ Fourth, aside from the keyboard and monitor, it had a number of I/O options.¹²⁴ Users could add a floppy disk drive or cassette tape device to store data and programs, connect a joystick or two paddles to play computer games, and produce sounds using the integrated speaker.¹²⁵ Fifth, it came with eight peripheral slots that made it possible to add

¹¹⁶ Steven Levy, *Hackers* 259.

¹¹⁷ Robert Cringely, *Accidental Empires* 62; Steven Levy, *Hackers* 272.

¹¹⁸ Robert Cringely, *Accidental Empires* 62; Steven Levy, *Hackers* 265; Steve Wozniak “Foreword” in J Sather *Understanding the Apple II*.

¹¹⁹ James Fielding Sather, *Understanding the Apple II* 1-7; Steven Levy, *Hackers* 266 and 270.

¹²⁰ Steven Levy, *Hackers* 266.

¹²¹ James Fielding Sather, *Understanding the Apple II* 1-5 and 1-10.

¹²² James Fielding Sather, *Understanding the Apple II* 1-5.

¹²³ James Fielding Sather, *Understanding the Apple II* 1-1.

¹²⁴ James Fielding Sather, *Understanding the Apple II* 1-8; Robert Cringely, *Accidental Empires* 62.

¹²⁵ James Fielding Sather, *Understanding the Apple II* 1-8 and 1-10.

and further expand the computer's capabilities.¹²⁶ The expansion slots were designed pursuant to an open architecture that allowed other manufacturers to build compatible peripherals and accessories for the Apple II.¹²⁷ Unlike the Altair, the Apple II was not only hackable, but user-friendly as well.

The Apple II, which finally brought computing to the masses, confirmed the widely held belief of many hackers that “most problems could be solved if only people could get together, communicate, and share solutions”.¹²⁸ According to Levy,

It was the fertile atmosphere of Homebrew that guided Steve Wozniak through the incubation of the Apple II. The exchange of information, the access to esoteric technical hints, the swirling creative energy, and the chance to blow everybody's mind with a well-hacked design or program...¹²⁹

made it possible to create a computer that fundamentally changed society. The club was an ideal place for hardware hackers like Wozniak because they could engage in creative experimenting with electronics as well as a bit of socializing with other technically minded people.¹³⁰ Wozniak, who attended the very first meeting of Homebrew in Moore's garage, joined the club primarily because he wanted to learn more about computers and to build his own.¹³¹ The creative, free spirited and communal environment suited Wozniak since his main purpose for building a computer was not for any commercial or profit-making purpose but simply to have fun and show it to his friends – a hobby.¹³² Like the original MIT hackers, together with the joy of doing and making things, it was peer recognition and being

¹²⁶ James Fielding Sather, *Understanding the Apple II* 1-4 and 1-9.

¹²⁷ Steven Levy, *Hackers* 266.

¹²⁸ Steven Levy, *Hackers* 197.

¹²⁹ Steven Levy, *Hackers* 259.

¹³⁰ Steven Levy, *Hackers* 252.

¹³¹ Steven Levy, *Hackers* 252; John Markoff, *What the Dormouse Said* 276.

¹³² Steven Levy, *Hackers* 256; Steve Wozniak “Foreword” in J Sather *Understanding the Apple II*; Pekka Himanen, “A Brief History of Computer Hackerism” 188.

considered a great hacker that motivated him the most.¹³³ Wozniak thrived within the “gift economy” or “gift culture” of Homebrew where everyone is expected to “[b]ring back more than you take”.¹³⁴ As he received suggestions from other members on how to improve the computer he was developing, he freely shared the schematics of the board and monitor he created and gave away the source code of his programs.¹³⁵ As Sather explains,

...Wozniak was not a lone talent working in solitude at his cerebral pastime. He was a member of the Homebrew Computer Club, the club to end all clubs, from whose membership rolls have come several microcomputer industry leaders. His friends were very interested in Steve’s Apple and made substantial contributions to the Apple.¹³⁶

Like other inventions, the Apple II was in truth not the creation of a single person (although Steve Wozniak’s technical genius was an essential element) but it was a result of many people building on the work of others and various innovations coming together or developing on top of each other.¹³⁷ The Apple II was the product of Wozniak’s inventiveness as well as the culture of openness, sharing and collaboration that was hardwired into the Homebrew Computer Club.

2.2.2.4 Blue boxes and paper tapes

In general, the interactions and dealings of computer hobbyists with the law in the 1970s were few and far between. Like the dominant technology companies at the time that made mainframe computers and calculators, the authorities considered the activities and creations

¹³³ Steven Levy, *Hackers* 264; Eric Raymond, “A Brief History of Hackerdom” 204.

¹³⁴ John Markoff, *What the Dormouse Said* 281; see also Eric Raymond, “A Brief History of Hackerdom” 204.

¹³⁵ Steven Levy, *Hackers* 257-258; Robert Pool, “A History of the Personal Computer” 92; Pekka Himanen, “A Brief History of Computer Hackerism” 188.

¹³⁶ James Fielding Sather, *Understanding the Apple II H-1*; see also John Markoff, *What the Dormouse Said* 282.

¹³⁷ Steven Levy, *Hackers* 259; but see Robert Cringely, *Accidental Empires* 62.

of computer hobbyists as trivial or innocuous and not worth their serious attention.¹³⁸ However, there were two cases that would portend the escalating conflicts between hacking and law.

The first incident involved “phone phreaking”, which is defined as the “art and science of cracking the phone network (so as, for example, to make free long-distance calls)”.¹³⁹ The phone phreaker subculture was based on a simple but powerful hack. They discovered, among other things, that “the whistle that came in the Cap’n Crunch cereal box was tuned to the precise [2,600] frequency that enabled it to control the long-distance calling switches of the AT&T telephone network”.¹⁴⁰ Phreakers could simply whistle into a telephone and then have the ability to make calls to anywhere in the world free of charge.¹⁴¹ When the exploits of the phone phreakers, particularly Captain Crunch (who was John Draper, a member of the Homebrew Computer Club), gained public attention after an article about them appeared in *Esquire* magazine, Captain Crunch became the target of both hackers and law enforcement.¹⁴² Hackers were interested in learning from him how phone phreaking worked, while the telephone companies wanted him stopped or apprehended. Steve Wozniak and Steve Jobs were able to find out who Captain Crunch was and he taught them “the art of building their own blue boxes, devices that were capable of gaining free – and illegal – access to the phone network”.¹⁴³ Before they started the company Apple, Wozniak and Jobs “built their own [blue boxes], and not only used them to make free calls but at one point sold them door-to-door at the Berkeley dorms”.¹⁴⁴ There was even an incident where the pair were caught

¹³⁸ See Steven Levy, *Hackers* 188 and 259; Pekka Himanen, “A Brief History of Computer Hackerism” 187.

¹³⁹ “Phreaking”, *The New Hacker’s Dictionary*.

¹⁴⁰ John Markoff, *What the Dormouse Said* 271; see also Steven Levy, *Hackers* 253.

¹⁴¹ Sherry Turkle, *The Second Self* 207; John Soma and others, “Legal Analysis of Electronic Bulletin Board Activities” 573.

¹⁴² John Markoff, *What the Dormouse Said* 272; Steven Levy, *Hackers* 255.

¹⁴³ John Markoff, *What the Dormouse Said* 272; see also Bruce Sterling, *The Hacker Crackdown* 54; see also Ken Lindup, “The Cyberpunk Age” 638 (for other kinds of boxes that phreakers made).

¹⁴⁴ Steven Levy, *Hackers* 251; see also Bruce Sterling, *The Hacker Crackdown* 54.

red-handed with a blue box but they were able to convince the police that it was an electronic music synthesizer.¹⁴⁵ Captain Crunch was not so lucky. He was arrested, convicted and served time for phone fraud a number of times.¹⁴⁶ However, despite his arrest and conviction, he continued to share his knowledge of the secrets of phone phreaking because “he was unable to resist when people asked; the hacker in his blood just let the information flow”.¹⁴⁷

The case of phone phreaking is indicative of the deep-seated and uneasy tension between the need of hackers to explore, learn about technologies and make a change in the world and the desire of commercial interests and the authorities to keep their systems safe, protected and under their control. It is worth emphasizing that the motivation of most phone phreakers, including Captain Crunch, was to freely explore and learn how the worldwide telecommunications network worked rather than to make phone calls and not pay for them.¹⁴⁸ According to *The New Hacker’s Dictionary*: “At one time phreaking was a semi-respectable activity among hackers; there was a gentleman’s agreement that phreaking as an intellectual game and a form of exploration was OK, but serious theft of services was taboo”.¹⁴⁹ Sterling recounts that “in the early days of phreaking, blue-boxing was scarcely perceived as ‘theft’, but rather as a fun (if sneaky) way to use excess phone capacity harmlessly”.¹⁵⁰ Phone phreaking was about free as in freedom, not free calls.¹⁵¹ Captain Crunch explains his fascination with phreaking:

¹⁴⁵ Phil Lapsely, “The Definitive Story of Steve Wozniak, Steve Jobs, and Phone Phreaking”.

¹⁴⁶ John Markoff, *What the Dormouse Said* 272.

¹⁴⁷ Steven Levy, *Hackers* 255-256; see also Bruce Sterling, *The Hacker Crackdown* 62.

¹⁴⁸ Ron Rosenbaum, “Secrets of the Little Blue Box” 120; but see Steven Levy, *Hackers* 251 (Steve Wozniak and Steve Jobs built and sold blue boxes for profit)

¹⁴⁹ “Phreaking”, *The New Hacker’s Dictionary*; see also Bruce Sterling, *The Hacker Crackdown* 52; see also Reid Skibell, “Cyber-crimes & Misdemeanors” 937.

¹⁵⁰ Bruce Sterling, *The Hacker Crackdown* 54.

¹⁵¹ See “The Free Software Definition” <<http://www.gnu.org/philosophy/free-sw.html>> accessed 2 July 2013 (the free and open source software movement defines “free” in the sense of “‘free’ as in ‘free speech,’ not as in ‘free beer’”).

... I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System... If I do what I do, it is only to explore a System. Computers. Systems. That's my bag. The phone company is nothing but a computer.¹⁵²

Levy similarly recounts how another member of Homebrew “would use the box [which Wozniak and Captain Crunch helped him make] only for connecting to the computer – a practice which in the hacker mind justifies lawbreaking – and not for personal gain in trivial matters like calling distant relatives”.¹⁵³ When one considers that a significant number of the top phone phreakers in the 1970s were visually impaired, freedom to connect and access were their primary objectives and not to steal services or defraud phone companies.¹⁵⁴ For people who are highly dependent on telephones to keep in touch with and reach out to the outside world, long-distance phone charges were a significant barrier to accessibility.¹⁵⁵ Of course, phone phreaking was considered a form of telecommunications fraud under the law and phone companies lost revenues due to this activity.

The second incident concerned intellectual property rights and the “theft” of software. Like the MIT hackers who originally had their “paper tapes in a drawer, a collective program library where you’d have people use and improve your programs”, many computer hobbyists freely shared the software they and others wrote.¹⁵⁶ The rationale was “computers belonged not to individuals but to the world of users”.¹⁵⁷ The free sharing, copying, modification, access to and use of software were an integral part of the hobbyist culture. However, people like Bill Gates saw the potential of computers to create great economic and

¹⁵² Ron Rosenbaum, “Secrets of the Little Blue Box” 120; see also Steven Levy, *Hackers* 254; see also Sherry Turkle, *The Second Self* 208; see also Bruce Sterling, *The Hacker Crackdown* 53.

¹⁵³ Steven Levy, *Hackers* 256.

¹⁵⁴ Ron Rosenbaum, “Secrets of the Little Blue Box” 120; Phil Lapsley, *Exploding the Phone*.

¹⁵⁵ Phil Lapsley, *Exploding the Phone*.

¹⁵⁶ Steven Levy, *Hackers* 118.

¹⁵⁷ Steven Levy, *Hackers* 118.

social value as part of a commercial enterprise.¹⁵⁸ After learning about the Altair, Bill Gates famously left Harvard to start with his friend Paul Allen a software company then called Micro-Soft in Albuquerque, New Mexico near the MITS factory.¹⁵⁹ Gates and Allen wrote a version of the BASIC computer language to run on the Altair (Altair BASIC), which was sold by MITS.¹⁶⁰ During an Altair traveling exhibition in a hotel in Palo Alto, California, some Homebrew Computer Club members spotted an Altair running an unreleased version of Altair BASIC (which was stored on paper tapes).¹⁶¹ Someone decided to “borrow” a paper tape and asked another Homebrew member, Dan Sokol, to make copies.¹⁶² At the next Homebrew meeting, Sokol brought over seventy copies and shared them for free with club members.¹⁶³ True to the collectivist spirit of hobbyists, “The only stipulation was that if you took a tape, you should make copies and come to the next meeting with two tapes. And give them away”.¹⁶⁴ Hobbyists believed they were not stealing information as much as they were liberating it.¹⁶⁵ There were a number of reasons hobbyists used to justify their possession of “pirated” copies of Altair BASIC (MITS was greedy and the price of the software was too high, they had already pre-ordered and paid for the product from MITS anyway, etc.), but many agreed “it seemed right to copy”.¹⁶⁶ In the mind of the computer hobbyists, “Why should there be a barrier of ownership standing between a hacker and a tool to explore, improve, and build systems?”¹⁶⁷

When copies of Altair BASIC began to circulate in Homebrew and other computer clubs around the country, Gates and Allen were incensed since they only received royalties from MITS when a copy of

¹⁵⁸ Steven Levy, *Hackers* 228.

¹⁵⁹ John Markoff, *What the Dormouse Said* 284; Robert Cringely, *Accidental Empires* 54-55.

¹⁶⁰ Steven Levy, *Hackers* 229.

¹⁶¹ Steven Levy, *Hackers* 231.

¹⁶² Steven Levy, *Hackers* 231; John Markoff, *What the Dormouse Said* 284.

¹⁶³ Steven Levy, *Hackers* 232; John Markoff, *What the Dormouse Said* 284-285.

¹⁶⁴ Steven Levy, *Hackers* 232.

¹⁶⁵ Steven Levy, *Hackers* 230-232.

¹⁶⁶ Steven Levy, *Hackers* 232; see also John Markoff, *What the Dormouse Said* 285.

¹⁶⁷ Steven Levy, *Hackers* 232.

the program was sold.¹⁶⁸ Gates wrote a letter entitled “Open Letter to Hobbyists” which was published in a number of publications and newsletters including the Homebrew Computer Club’s.¹⁶⁹ In his letter, Gates accused computer hobbyists of being thieves because most of them used software that they did not pay for or lawfully acquire (“As the majority of hobbyists must be aware, most of you steal your software” and “Most directly, the thing you do is theft”).¹⁷⁰ He pointed out the incongruity of the fact that “Hardware must be paid for, but software is something to share. Who cares if the people who worked on it get paid?”¹⁷¹ Interestingly, Gates argued against the ability of the cooperation and sharing model to produce useful innovation:

One thing you do do is prevent good software from being written. Who can afford to do professional work for nothing? What hobbyist can put 3-man years into programming, finding all bugs, documenting his product and distribute for free? The fact is, no one besides us has invested a lot of money in hobby software...., but there is very little incentive to make this software available to hobbyists.¹⁷²

The law was never brought in to resolve the matter despite the fact that copyright protection over computer programs was recognized under the amendments to the US Copyright Act of 1976.¹⁷³ Gates’s letter, however, produced ill feelings among computer hobbyists and, more importantly, this “software flap” and the success of the Apple II signaled a turning point in the culture and outlook of the community.

174

¹⁶⁸ Steven Levy, *Hackers* 232; John Markoff, *What the Dormouse Said* 285.

¹⁶⁹ Steven Levy, *Hackers* 232-233.

¹⁷⁰ Bill Gates, “Open Letter to Hobbyists”; see also Robert Cringely, *Accidental Empires* 55; see also Forrest Mims III, “The Tenth Anniversary of the Altair 8800” 81 (“Without intending to, MITS made software piracy a widespread phenomenon”).

¹⁷¹ Bill Gates, “Open Letter to Hobbyists”.

¹⁷² Bill Gates, “Open Letter to Hobbyists”.

¹⁷³ See E. Gabriella Coleman, *Coding Freedom* 67; Sam Williams, *Free As In Freedom* 106.

¹⁷⁴ Steven Levy, *Hackers* 233 and 265; see also Sam Williams, “Free As In Freedom” 89.

2.2.2.5 Free and open versus proprietary and closed

As computer technologies and the computer market began to mature, hobbyists gradually realized that they could make real money from and exert ownership over their innovations.¹⁷⁵ Levy recounts how “the pioneers of Homebrew... switched from building computers to manufacturing computers.... It retarded Homebrew’s time-honored practice of sharing all techniques, of refusing to recognize secrets, and of keeping information going in an unencumbered flow”.¹⁷⁶ Their focus had shifted from promoting freedoms that were essential for hacking to protecting (intellectual) property rights.

The split in the hobbyist community between hackers and entrepreneurs seems inevitable given the increasing commercial value of technologies and intellectual property and the widening distribution and impact of computers.¹⁷⁷ A similar shift occurred with the computer hackers at MIT where commercialism and the assertion of exclusive intellectual property rights over their hardware and software creations virtually exorcised the hacker spirit from its hallowed halls.¹⁷⁸ As the first hacker generations created their own companies and sought to develop and protect their proprietary technologies, barriers to sharing and collaboration were erected.¹⁷⁹ As Levy explains:

But even if people in the company were speaking to each other, they could not talk about what mattered most – the magic they had discovered and forged inside the computer systems. The magic was now a trade secret, not for examination by competing firms. By working for companies, the members of the purist hacker society had discarded the key element in the Hacker Ethic: the free flow of information.¹⁸⁰

¹⁷⁵ Steven Levy, *Hackers* 264; Paul Taylor, “From hackers to hacktivists” 629.

¹⁷⁶ Steven Levy, *Hackers* 276.

¹⁷⁷ Robert Cringely, *Accidental Empires* 55; John Markoff, *What the Dormouse Said* 286.

¹⁷⁸ Steven Levy, *Hackers* 441-442.

¹⁷⁹ Steven Levy, *Hackers* 442; E. Gabriella Coleman, *Coding Freedom* 68.

¹⁸⁰ Steven Levy, *Hackers* 277 and 442-447 (for an account of the LISP machine conflict); see Sam Williams, “Free As In Freedom” 83-87 (who provides details on how the LISP machine conflict that divided the hackers at the MIT Artificial Intelligence Lab developed)

The initial openness and then gradual closure of technology seem to be an enigmatic property of the history of information and communications technology as well as hacking.¹⁸¹ As illustrated above, a host of legal, technical and social factors and conditions contributed to or facilitated this vacillation between the opening and closing of hacker communities and their technologies. This peculiar nature of innovation may be partly explained by Stewart Brand's famous observation about the innate and paradoxical tendency of information to move in two opposite directions:

Information wants to be free because it has become so cheap to distribute, copy, and recombine – too cheap to meter. It wants to be expensive because it can be immeasurably valuable to the recipient. That tension will not go away. It leads to endless wrenching debate about price, copyright, 'intellectual property', the moral rightness of casual distribution, because each round of new devices makes the tension worse, not better.¹⁸²

The same dynamic has played out between and among hackers. Dyed-in-the-wool, purist hackers like Wozniak aimed to make a difference with and through technology and shared their creations freely, whereas Gates and entrepreneurial hobbyists desired to change the world by commercializing their innovations, building companies and transforming entire industries.¹⁸³ This push-and-pull between the free and open versus the proprietary and closed philosophies to developing and distributing technologies split apart the early generations of hackers and continues to divide hacker culture today.¹⁸⁴ For better or worse, both open and closed models profoundly shaped the face of computing and would help diffuse the technologies, norms and values of hackers to the world at large through the next generations of hackers.

¹⁸¹ See Tim Wu, *The Master Switch*.

¹⁸² See Stewart Brand, *The Media Lab 202* (emphasis added).

¹⁸³ Steven Levy, *Hackers* 264.

¹⁸⁴ John Markoff, *What the Dormouse Said* 287; see Rob Giseburt "Is One of Our Open Source Heroes Going Closed Source?"

The PC revolution, which began in the late 1970s, brought computing out of laboratories and corporate computer rooms and into more people's hands, homes and workspaces.¹⁸⁵ It comes as no surprise that the widespread distribution and use of computers gave rise to two influential types of hackers in 1980s – underground hackers and free and open source software (FOSS) developers. These distinct hacker types will be discussed separately but it should be noted that they more or less inhabited the same historical and temporal milieu.

2.2.3 OF PERSONAL COMPUTERS, MODEMS AND BEDROOMS – UNDERGROUND HACKERS

2.2.3.1 Bulletin Board Systems

A modern, general-purpose PC,¹⁸⁶ together with a modem and a telephone line, would open the doors for and become the tools of choice of a new generation of hackers. Underground hackers were not only keen on understanding the inner workings of their PCs but they used these technologies to connect with other people, computers and networks. In the United States, these mostly white, male teenagers and university students from middle-class backgrounds sought to establish their own unique identity and community and explore the vast electronic world of computer systems and telecommunications networks without interference from any authority or the expectations and rules of society.¹⁸⁷ Technological developments afforded them the ability to pursue these goals without having to physically leave the comfort of their homes and bedrooms.¹⁸⁸

¹⁸⁵ See Reid Skibell, "The Myth of the Computer Hacker" 340.

¹⁸⁶ The term "PC" is used as a generic term and is not limited to IBM PCs and computers based on the "Wintel" architecture that gained market dominance in the late 1980s and 1990s. Notable PCs that came after the Apple II include the TRS-80, Atari 400 and 800, Commodore PET and 64, BBC Micro, Sinclair ZX Spectrum, and, most importantly, the IBM PC and the Apple Macintosh.

¹⁸⁷ See Bruce Sterling, *The Hacker Crackdown* 63-65 and 90; Douglas Thomas, *Hacker Culture* xiii; John Soma and others, "Legal Analysis of Electronic Bulletin Board Activities" 574; Debora Halbert, "Discourses of Danger and the Computer Hacker" 363; Reid Skibell, "The Myth of the Computer Hacker" 340; Richard Hollinger, "Hackers: Computer Heroes or Electronic Highwaymen?" 12; Ken Lindup, "The Cyberpunk Age" 638.

¹⁸⁸ Bruce Sterling, *The Hacker Crackdown* 54 and 81; Damian Gordon, "Forty Years of Movie Hacking" 25.

The electronic Bulletin Board System (BBS) was at the heart of the underground hacker community.¹⁸⁹ BBSes (or simply boards) were “the life-blood of the digital underground” and figured prominently in the many clashes between underground hackers and the law.¹⁹⁰ A BBS is defined in *The New Hacker’s Dictionary* as “a message database where people can log in and leave broadcast messages for others grouped (typically) into topic groups”.¹⁹¹ Sterling explains how a BBS works:

A “bulletin board system” can be formally defined as a computer which serves as an information and message-passing center for users dialing-up over the phone-lines through the use of modems. A “modem,” or modulator-demodulator, is a device which translates the digital impulses of computers into audible analog telephone signals, and vice versa. Modems connect computers to phones and thus to each other.¹⁹²

BBSes acted “as an electronic message center, and as a software library”.¹⁹³ In essence, a BBS was a medium for sending and receiving messages as well as for storing and exchanging information, programs and other data between people and computers located in different parts of the country and even all over the world.¹⁹⁴ During the 1980s, there were three basic types of BBSes: private computer boards that were used internally by private entities; commercial boards run by companies that the general public could access for a fee; and free boards that did not charge for access and were run by systems operators (sysops) as a hobby out of their homes.¹⁹⁵ The BBS could be considered a forerunner of online discussion forums, chat rooms and

¹⁸⁹ Tim Jordan, *Hacking* 37.

¹⁹⁰ Bruce Sterling, *The Hacker Crackdown* 69; see also Tatiana Bazzichelli, *Networking: The Net as Artwork* 136.

¹⁹¹ “BBS”, *The New Hacker’s Dictionary*.

¹⁹² Bruce Sterling, *The Hacker Crackdown* 69; see also John Soma and others, “Legal Analysis of Electronic Bulletin Board Activities” 572.

¹⁹³ Charles Cangialosi, “The Electronic Underground: Computer Piracy and Electronic Bulletin Boards” 267.

¹⁹⁴ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 499 and 501; Bruce Sterling, *The Hacker Crackdown* 70; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 217; Charles Cangialosi, “The Electronic Underground: Computer Piracy and Electronic Bulletin Boards” 283.

¹⁹⁵ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 500-501; Bruce Sterling, *The Hacker Crackdown* 69; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 221.

social networking sites.¹⁹⁶

Boards had particular attributes that made them appropriate domains of and instruments for the activities and communications of underground hackers, who, by and large, espoused libertarian and anti-establishment sentiments.¹⁹⁷ A BBS could be considered a prime example of “democratized technology”¹⁹⁸ since the barriers to entry were low and “anybody with a computer, modem, software and a phone-line can start a board”.¹⁹⁹ A basic board was relatively simple and inexpensive to get up and running.²⁰⁰ According to Beall, “The entire cost of the initial set-up can be as little as \$2,000”.²⁰¹ Furthermore, under US telecommunications law, BBSes were considered “enhanced services” and thus not subject to regulation or supervision by the US Federal Communications Commission (FCC) and other governmental bodies.²⁰² Despite their virtual character, another important feature of boards was the breadth and extent of their territorial influence.²⁰³ BBSes could reach a national and even global audience since “[b]oards can be contacted from anywhere in the global telephone network, at NO COST to the person running the board – the caller pays the phone bills, and if the caller is local, the call is free”.²⁰⁴ BBSes were also extremely user-friendly. To access a board, users simply used their computers and modems to call the telephone number of a specific BBS and, once connected, log in using their usernames and passwords.²⁰⁵

¹⁹⁶ See Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 499.

¹⁹⁷ Bruce Sterling, *The Hacker Crackdown* 64 and 73; Tim Jordan, *Hacking* 38; John Raulerson, “Cyberpunk Politics: Hacking and Bricolage” 122.

¹⁹⁸ See Andrew Feenberg, “Democratizing Technology: Interest, Codes, Rights” 192-193; see Eric von Hippel, *Democratizing Innovation* 1; Chris Anderson, *Makers* 63.

¹⁹⁹ Bruce Sterling, *The Hacker Crackdown* 70.

²⁰⁰ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 501; see Bruce Sterling, *The Hacker Crackdown* 70.

²⁰¹ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 501; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 220.

²⁰² Bruce Sterling, *The Hacker Crackdown* 70; see also Eric Jensen, “Computer Bulletin Boards and the First Amendment” 219-220.

²⁰³ Eric Jensen, “Computer Bulletin Boards and the First Amendment” 222.

²⁰⁴ Bruce Sterling, *The Hacker Crackdown* 70.

²⁰⁵ See Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 499-500; see Bruce Sterling, *The Hacker Crackdown* 71; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 218.

BBSes were effectively a marketplace of ideas since the tens of thousands of boards that were created covered all conceivable topics and subject areas from pedestrian to fringe interests.²⁰⁶ The free and open exchange of ideas and information was bolstered by the fact that boards “[offered] instant, multiple, interactive communications”²⁰⁷ and supported anonymous and pseudonymous speech (users could employ made up usernames instead of their real names).²⁰⁸ Of course, since sysops were themselves technically inclined, a majority of boards were about computers, phones, networks, hardware, software, and services.²⁰⁹

2.2.3.2 The digital underground

The computer hackers and phone phreakers who made up the digital underground reveled in and thrived under the virtually limitless freedom and liberty offered by boards, especially the underground or hacker boards that they constructed for themselves.²¹⁰ They built communities and spread the hacker culture not just “in there” (in the computer) but, more importantly, “out there” in the growing networks of linked computers and telephone connections. What primarily distinguished underground boards from normal BBSes was the high degree of secrecy and pseudo-anonymity of and among users and their involvement with what the law and society would consider restricted, illicit or off limit topics, content and activities.²¹¹ Underground hacker groups in the United States went by catchy, provoking and exaggerated names such as “Cult of the Dead Cow”, “Phreaks and Hackers of America” and “Legion of Doom”.²¹² They also deliberately

²⁰⁶ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 501; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 222; Bruce Sterling, *The Hacker Crackdown* 73.

²⁰⁷ Eric Jensen, “Computer Bulletin Boards and the First Amendment” 223.

²⁰⁸ Bruce Sterling, *The Hacker Crackdown* 70-71 and 76; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 223-224; Charles Cangialosi, “The Electronic Underground: Computer Piracy and Electronic Bulletin Boards” 276.

²⁰⁹ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 501; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 222; Bruce Sterling, *The Hacker Crackdown* 73.

²¹⁰ Bruce Sterling, *The Hacker Crackdown* 73; John Soma and others, “Legal Analysis of Electronic Bulletin Board Activities”.

²¹¹ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 502; Paul Taylor, *Hackers* 28; Tim Jordan, *Hacking* 33-34.

²¹² Bruce Sterling, *The Hacker Crackdown* 74-75

used intriguing pseudonyms (handles) and, tongue-in-cheek, portrayed themselves to the outside world as “punks, gangs, delinquents, mafias, pirates, bandits and racketeers”.²¹³

In and through boards, underground hackers “mainly and habitually communicated with each other in a disembodied, text-based environment about fast-changing technologies”.²¹⁴ They communicated about topics that interested them the most – “hardware, software, sex, science fiction, current event, politics, movies, personal gossip”.²¹⁵ Using the BBS’s function as a software library, they created and shared what they considered exciting “forbidden knowledge” that needed to be openly accessed by everyone and distributed as widely as possible, such as copies of electronic underground magazines like Phrack and “philes”, which were “pre-composed texts which teach the techniques and ethos of the underground” like “do-it-yourself manuals about computer intrusion”.²¹⁶ Underground BBSes also contained software and computer games (whether legitimately owned or the pirated, cracked variety),²¹⁷ copies of manuals, books and other printed materials,²¹⁸ long distance access codes and telephone credit card numbers,²¹⁹ and other kinds of computer intrusion information.²²⁰ They engaged in various forms of hacking: they explored and learned about the intricacies of computer and telecommunications networks and did not hesitate to break any security measures that were in their way; they kept themselves secure by using techniques that concealed their identities and activities; and they discovered and created new technical hacks and exploits and shared them with others on BBSes.

²¹³ Bruce Sterling, *The Hacker Crackdown* 75 and 78; see also Tim Jordan, *Hacking* 33-34.

²¹⁴ Tim Jordan, *Hacking* 29.

²¹⁵ Bruce Sterling, *The Hacker Crackdown* 77.

²¹⁶ Bruce Sterling, *The Hacker Crackdown* 77-79, 85 and 87; see also Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 502.

²¹⁷ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 502; Bruce Sterling, *The Hacker Crackdown* 80.

²¹⁸ Bruce Sterling, *The Hacker Crackdown* 80.

²¹⁹ Robert Beall, “Developing a Coherent Approach to the Regulation of Computer Bulletin Boards” 502; Eric Jensen, “Computer Bulletin Boards and the First Amendment” 225.

²²⁰ Eric Jensen, “Computer Bulletin Boards and the First Amendment” 225; John Soma and others, “Legal Analysis of Electronic Bulletin Board Activities” 574.

Underground hackers did not see their activities as “deviant behavior, but instead, the symbolic expression of their hostility to all large bureaucratic organizations that control informational or communications resources”.²²¹

Like the early computer hackers and computer hobbyists, underground hackers were generally not interested in stealing information or causing damage to technical systems.²²² According to sociological research, “hackers have diverse motivations” and they were generally “driven by more benign motivations such as curiosity, feelings of power, and the camaraderie of belonging to a community”.²²³ One of their primary motivations was to build a reputation for technological wizardry among peers and the wider underground community.²²⁴ Because of this, “[t]he main reason that hackers do not intentionally damage networks or commit fraud is a type of communal boundary formation. Hackers do not see themselves as criminals and enforce a code of conduct that functions as a form of self-regulation”.²²⁵

However, hackers are not irreproachable and some form of personal or pecuniary benefit can be derived from hacking. As Sterling points out,

a big reputation in the digital underground did not coincide with one’s willingness to commit “crimes”. Instead reputation was based on cleverness and technical mastery. As a result, it often seemed that the HEAVIER the hackers were, the LESS likely they were to have committed any kind of common, easily prosecutable crime. There were some hackers who could really steal. And there were hackers who could really hack. But the two groups didn’t seem to overlap much, if at all.

²²¹ Richard Hollinger, “Hackers: Computer Heroes or Electronic Highwaymen?” 9.

²²² John Soma and others, “Legal Analysis of Electronic Bulletin Board Activities” 574; David Wall, *Cybercrime* 55; Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 581; Reid Skibell, “Cybercrimes & Misdemeanors” 936-937.

²²³ Reid Skibell, “Cybercrimes & Misdemeanors” 937; see also Paul Taylor, *Hackers*; see also Tim Jordan and Paul Taylor, “A sociology of hackers”.

²²⁴ Bruce Sterling, *The Hacker Crackdown* 90; Reid Skibell, “The Myth of the Computer Hacker” 341.

²²⁵ Reid Skibell, “Cybercrimes & Misdemeanors” 937; see also Tim Jordan, *Hacking*; see also Paul Taylor, *Hackers*; see also Michelle Slatalla and Joshua Quittner, *Masters of Deception*.

Truly heavy-duty hackers, those with serious technical skills who had earned the respect of the underground, never stole money or abused credit cards. Sometimes they might abuse phone-codes – but often, they seemed to get all the free phone-time they wanted without leaving a trace of any kind.

The best hackers, the most powerful and technically accomplished, were not professional fraudsters. They raided computers habitually, but wouldn't alter anything, or damage anything.²²⁶

The principal aims of hacking were to freely explore and learn about computers and networks and to ensure that technologies remained free and open to all and independent from outside authority, control or interference.²²⁷ It was not about financial gain but freedom of access.²²⁸ For underground hackers, “computers and telephones [were] potent symbols of organized authority and the technocratic business elite”.²²⁹ They believed that “[s]ince access to information is power... control over the computer is yet another example of corporate and government oppression of the masses”.²³⁰ For example, the overriding reason why underground hackers dealt in long distance phone codes was because dialing to a BBS outside of their local area would mean incurring very prohibitive long-distance charges on the part of teenage and twenty-something hackers.²³¹ By and large, underground hackers exhibited the key characteristics of: “[seeking] access to forbidden knowledge...; fast turnover of members; small numbers but strongly interconnected communication; peer education; low-level and limited forms of formal organization; and a desire for exploration”.²³² Furthermore, they were obsessive about and placed a high value on technology, secrecy, anonymity and confrontation with authority.²³³

²²⁶ Bruce Sterling, *The Hacker Crackdown* 90 (emphasis added).

²²⁷ Bruce Sterling, *The Hacker Crackdown* 82; Wayne Rumbles, “Reflections of Hackers in Legal and Popular Discourse” 75; Richard Hollinger, “Hackers: Computer Heroes or Electronic Highwaymen?” 11-12.

²²⁸ Reid Skibell, “Cybercrimes & Misdemeanors” 919 and 937.

²²⁹ Bruce Sterling, *The Hacker Crackdown* 54.

²³⁰ Richard Hollinger, “Hackers: Computer Heroes or Electronic Highwaymen?” 9.

²³¹ Bruce Sterling, *The Hacker Crackdown* 80-81; Richard Hollinger, “Hackers: Computer Heroes or Electronic Highwaymen?” 9; Ken Lindup, “The Cyberpunk Age” 639.

²³² Tim Jordan, *Hacking* 28-30.

Unlike their hands-off approach to the early hacker generations, the authorities did not turn a blind eye to the happenings in the digital underground.²³⁴ Rather than tolerating the activities of underground hackers, beginning in the 1980s, governments around the world enacted computer crime laws that prohibited many forms of hacking and intensified law enforcement activities against these acts.²³⁵ Some argue that the “timing of criminalization corresponds more closely to the public availability of personal computers and telephone modems than to the introduction of computerized data processing or abuse”.²³⁶ It also took time for government actors to become fully aware of the legal and social impact of hacking and other technical developments. Nissenbaum goes much further and believes that the “changes in the popular conception of hacking have as much to do with changes in specific background conditions, changes in the meaning and status of the new digital media, and the powerful interests vested in them, as with hacking itself”.²³⁷ While the pseudo-menacing posturing of underground hackers and their feelings of invisibility and invincibility from authorities may have contributed to the public’s negative view of hacking,²³⁸ it was the “confluence of media attention, law enforcement and legislative reactions to that attention, and computer security vendors’ attempts to capitalize on” the fears, concerns and risks associated with hacking that ultimately resulted in hacking becoming a serious target of law, and underground hackers being depicted in and by the media as “a new villain, the ‘malicious hacker’”.²³⁹ These factors and

²³³ Tim Jordan, *Hacking* 28-29; Ken Lindup, “The Cyberpunk Age” 639.

²³⁴ Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 199-200.

²³⁵ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 581-582; Ian Lloyd, *Information Technology Law* 215; Tim Jordan, *Hacking* 39; Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 196; Debora Halbert, “Discourses of Danger and the Computer Hacker” 364; Reid Skibell, “The Myth of the Computer Hacker” 349.

²³⁶ Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 116.

²³⁷ Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 200; see also David Wall, *Cybercrime* 9-10.

²³⁸ Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 198; Bruce Sterling, *The Hacker Crackdown* 59, 62, 64, 91 and 96 (“Hackers weren’t ‘invisible’. They THOUGHT they were invisible; but the truth was, they had just been tolerated too long”); Reid Skibell, “The Myth of the Computer Hacker” 346; Tim Jordan, *Hacking* 19 and 39; Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 45.

²³⁹ Jay BloomBecker, “Computer Crime Update” 628 and 637; see also Debora Halbert, “Discourses of Danger and the Computer Hacker”; see also Reid Skibell, “The Myth of the Computer Hacker”; see also Paul Taylor, *Hackers* 1; see also Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 114-115.

conditions helped solidify the association of hacking to crime and deviance in the public’s mind.²⁴⁰ Skibell explains,

this new branding of the hacker as criminal was not imposed by any single entity, but rather was formed by a network of actors including hacker themselves. They were complicitous in their own branding as criminals, and in many ways helped create the public personae that the [computer security] industry thrived on and used to justify their own expertise.²⁴¹

The first hacker generations were dismayed that “the word hacker had acquired a specific and negative connotation” and “quickly became synonymous with ‘digital trespasser’”.²⁴² Other types of hackers “deeply resent[ed] the attack on their values implicit in using the word ‘hacker’ as a synonym for computer-criminal”.²⁴³ Even if other hackers preferred to distance themselves from the activities of and the negative publicity surrounding underground hackers, these “kids” not only called themselves “hackers” but they also drew from and considered themselves a part of hacker culture.²⁴⁴ The impact of the criminalization of hacking is discussed at length in Section 4.2.

2.2.4 OF FREE AND OPEN SOURCE SOFTWARE, LICENSES AND MOVEMENTS – FOSS DEVELOPERS

2.2.4.1 Free software

The enactment of computer crime laws and the stronger protection and enforcement of intellectual property rights from the 1980s onwards signaled the law’s formal and definitive entry into the world

²⁴⁰ Jay BloomBecker, “Computer Crime Update” 649; Ulrich Wuermeling, “Hacking for the KGB” 21; “A short history of the CCC” 86.

²⁴¹ Reid Skibell, “The Myth of the Computer Hacker” 346; see also Paul Taylor, *Hackers* xiii and 5; see also Reid Skibell, “Cybercrimes & Misdemeanors” 943.

²⁴² Steven Levy, *Hackers* 456; David Wall, *Cybercrime* 54; Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 44 and 45.

²⁴³ Bruce Sterling, *The Hacker Crackdown* 59; see also Reid Skibell, “Cybercrimes & Misdemeanors” 937.

²⁴⁴ Steven Levy, *Hackers* 456; Bruce Sterling, *The Hacker Crackdown* 59; see David Wall, *Cybercrime* 68.

²⁴⁵ See Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 584.

of hacking and computers.²⁴⁵ While computer crime laws were being used to prosecute members of the digital underground, commercial interests and the heightened concern for intellectual property rights were driving out the hacker ethic from the soul of computer hackers.²⁴⁶ Even the hacker paradise at MIT was not spared. By the early 1980s, most of the original MIT hackers had either started or joined businesses or commercial enterprises whose primary objective was to exploit computer technologies and innovations for profit.²⁴⁷

Hoping to preserve the freedoms of users and the openness of computers, Richard Stallman, who had been a hacker at the MIT Artificial Intelligence Laboratory since 1971, decided that creating a completely free computer operating system that was faithful to hacker values would help rebuild the “software-sharing community” of hackers.²⁴⁸ Developing a free operating system was essential because it is

the basis for everything else that will happen in the machine. And creating one is the ultimate challenge. When you create an operating system, you’re creating the world in which all the programs running the computer live – basically, you’re making up the rules of what’s acceptable and can be done and what can’t be done. Every program does that, but the operating system is the most basic. It’s like creating the constitution of the land that you’re creating, and all the other programs running on the computer are just common laws.²⁴⁹

In creating an operating system, Stallman was animated by the belief that society could be changed for the better through the simple writing of software code.²⁵⁰ For technical and practical reasons (e.g., flexibility, portability and ubiquity), Stallman chose to build an operating system that was compatible with Unix, an operating system that

²⁴⁶ E. Gabriella Coleman, *Coding Freedom* 61.

²⁴⁷ Steven Levy, *Hackers* 440 and 447; Richard Stallman, “The GNU Project” 17-18; Sam Williams, “Free As In Freedom” 81.

²⁴⁸ Richard Stallman, “The GNU Project” 17, 19 and 21; see also Sam Williams, “Free As In Freedom” 81.

²⁴⁹ Linus Torvalds and David Diamond, *Just for Fun* 75.

²⁵⁰ Tim Jordan, *Hacking* 43-44; see Linus Torvalds and David Diamond, *Just for Fun* 238.

²⁵¹ Eric Raymond, *The Cathedral and the Bazaar* 8; E. Gabriella Coleman, *Coding Freedom* 76; Linus Torvalds and David Diamond, *Just for Fun* 56; Bruce Sterling, *The Hacker Crackdown* 107.

was developed by Dennis Ritchie and Ken Thompson at Bell Labs in 1969.²⁵¹ Unix was originally free for third parties to use and modify but it was closed and commercialized in the 1980s by the company that owned the intellectual property rights to Unix.²⁵² Stallman called the project GNU, which “following a hacker tradition” was “a recursive acronym for ‘GNU’s Not Unix’”.²⁵³ As Stallman envisioned it, the GNU Project would produce a full operating system that included “command processors, assemblers, compilers, interpreters, debuggers, text editors, mailers and much more”.²⁵⁴ After announcing his plan for a “new UNIX implementation” on Usenet newsgroup in September 1983, Stallman resigned from MIT in January 1984 to devote himself to the development and advocacy of “free software”.²⁵⁵ In this way, the “last of the true hackers” had finally stepped out of “the ivory towers of academia [and] the blue-sky institutions of research”²⁵⁶ and sought to bring hacker culture and values in the form of free software to the wider world of ordinary computer users.²⁵⁷ Furthermore, unlike the early computer hackers and computer hobbyists, Stallman’s approach to free software and hacking was markedly political and ideological.²⁵⁸

To be considered free software, users of a computer program must possess all of the “four essential freedoms”:²⁵⁹

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.

²⁵² Richard Stallman, “The GNU Project” 19, 24 and 25; Sam Williams, “Free As In Freedom” 79, 93 and 112; Eric Raymond, *The Cathedral and the Bazaar* 12-14; Tim Jordan, *Hacking* 53; Bruce Sterling, *The Hacker Crackdown* 111-112.

²⁵³ Richard Stallman, “The GNU Project” 19; see also Linus Torvalds and David Diamond, *Just for Fun* 58.

²⁵⁴ Richard Stallman, “The GNU Project” 19 and 24; see also Sam Williams, “Free As In Freedom” 115.

²⁵⁵ Richard Stallman, “Initial Announcement”; see also Sam Williams, “Free As In Freedom” 79-80; see also Richard Stallman, “The GNU Project” 20; see also Eric Raymond, *The Cathedral and the Bazaar* 11.

²⁵⁶ Richard Stallman, “The GNU Project” 21 (It should be noted though that while Richard Stallman severed formal ties with MIT as an employee, he remained physically present at MIT and continued to use the facilities of the MIT AI Lab upon the invitation of the Lab’s head even after he resigned); Sam Williams, “Free As In Freedom” 90; Paul Taylor, “From hackers to hacktivists” 629.

²⁵⁷ Steven Levy, *Hackers* 170, 437, 461 and 465.

²⁵⁸ Sam Williams, “Free As In Freedom” 92; E. Gabriella Coleman, *Coding Freedom* 88.

²⁵⁹ “The Free Software Definition”.

- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.²⁶⁰

According to Stallman, the “free” in free software “is a matter of liberty, not price” and should be conceived of as “‘free’ as in ‘free speech,’ not as in ‘free beer’”.²⁶¹ Free software was the binary opposite of “proprietary software”, which was “any program that carried private copyright or end-user license that restricted copying and modification”.²⁶² The GNU Project was, therefore, both a means and an end to free software and to reestablish the values of community and cooperation among hackers.²⁶³

The idea and ideology of free software did not catch on right away.²⁶⁴ Stallman encountered a number of technical, legal and resource-related difficulties during the early years of the GNU Project especially in the development of a GNU compiler and a GNU version of Emacs (GNU Emacs), a text editor.²⁶⁵ These problems were expected given that Stallman faced a world where software development had undergone severe commercialization and legalization as manifested in proprietary software and the legal regime that supported it.²⁶⁶ At the time, the proprietary and closed mindset, which viewed computer programs as valuable assets protected under intellectual property laws and exploited and controlled commercially through restrictive software licenses, trade secrets and non-disclosure agreements, was decidedly

²⁶⁰ “The Free Software Definition”.

²⁶¹ “The Free Software Definition”; see also Richard Stallman, “The GNU Project” 20.

²⁶² Sam Williams, “Free As In Freedom” 89.

²⁶³ Richard Stallman, “The GNU Project” 19; E. Gabriella Coleman, Coding Freedom 70.

²⁶⁴ Sam Williams, “Free As In Freedom” 90-91; E. Gabriella Coleman, Coding Freedom 70-71.

²⁶⁵ Sam Williams, “Free As In Freedom” 91-92; Richard Stallman, “The GNU Project” 21; E. Gabriella Coleman, Coding Freedom 69-70.

²⁶⁶ See E. Gabriella Coleman, Coding Freedom 88.

dominant. It would take a truly great and inspired “hack” that brought to bear social, technical and legal knowledge and skills to transform the current state of affairs. Since hackers reside at the nexus of technology, society and, by the 1980s, law, they would be in a position to ignite and fan a revolution.

2.2.4.2 Copyleft

Stallman abhorred the idea of copyright or private ownership over software because it went against the culture of sharing and cooperation among hackers.²⁶⁷ He considered this “a personal affront as well as a significant cultural threat” since he “fundamentally viewed the sharing of source code as the bedrock supporting the hacker practices of inquisitive tinkering and collaboration... the end of sharing amounted to the end of hacking”.²⁶⁸ Stallman particularly disliked copyright notices because it meant that, rather than working with and building on the work of others, a programmer was asserting his or her own individual authorship and sole authority over the program to the exclusion of others.²⁶⁹ Williams explains that there were a number of arguments “that eventually softened Stallman’s resistance to software copyright notices”²⁷⁰ and copyright in general: first, copyright prevents computer programs from entering the public domain and thus precludes people from making derivatives of public domain works that are closed and proprietary;²⁷¹ second, a copyright notice may be seen as a form of attribution and recognition where, by publicly declaring that they are the authors, programmers expressly stake their reputation on their creations;²⁷² and, last and most importantly, a programmer can

²⁶⁷ Steven Levy, *Hackers* 441.

²⁶⁸ E. Gabriella Coleman, *Coding Freedom* 68.

²⁶⁹ Steven Levy, *Hackers* 441; Sam Williams, “Free As In Freedom” 106.

²⁷⁰ Sam Williams, “Free As In Freedom” 107.

²⁷¹ People can do anything with works in the public domain, including making derivatives of these works that are no longer freely accessible to the public; see “What is Copyleft?”; Sam Williams, “Free As In Freedom” 108.

²⁷² Sam Williams, “Free As In Freedom” 107.

²⁷³ Sam Williams, “Free As In Freedom” 107; see also Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 562.

use the flexibility offered by the copyright bundle of rights and freedom of contract to creatively “give away certain rights in exchange for certain forms of behavior on the part of the user”.²⁷³

In order to affirm and preserve important hacker norms and values as well as to preclude the mischief of GNU software becoming proprietary software,²⁷⁴ Stallman, together with other free software developers who had formed the non-profit Free Software Foundation in 1985,²⁷⁵ came up with a simple but paradigm-changing solution, which they called copyleft: “users would be free to modify [free software] just so long as they published their modifications. In addition, the resulting ‘derivative’ works would also have [to] carry the same [free software license]”.²⁷⁶ As Stallman explains,

Copyleft uses copyright law, but flips it over to serve the opposite of its usual purpose: instead of a means of privatizing software, it becomes a means of keeping software free. The central idea of copyleft is that we give everyone permission to run the program, copy the program, modify the program, and distribute modified versions – but not permission to add restrictions of their own. Thus, the crucial freedoms that define “free software” are guaranteed to everyone who has a copy; they become inalienable rights.

77

GNU Emacs, the GNU Project’s first software that was generally available to the public, was released in 1985 under the GNU Emacs General Public License, which contained copyleft license provisions.²⁷⁸ The GNU Emacs software license explained:

GNU Emacs is free; this means that everyone is free to use it and free to redistribute it on a free basis. GNU Emacs is not in

²⁷⁴ Richard Stallman, “The GNU Project” 22; Sam Williams, “Free As In Freedom” 108.

²⁷⁵ Sam Williams, “Free As In Freedom” 93; Richard Stallman, “The GNU Project” 23; E. Gabriella Coleman, *Coding Freedom* 68.

²⁷⁶ Sam Williams, “Free As In Freedom” 107-108 and 111; see also Richard Stallman, “The GNU Project” 22.

²⁷⁷ Richard Stallman, “The GNU Project” 22.

²⁷⁸ Sam Williams, “Free As In Freedom” 93 and 108.

the public domain; it is copyrighted and there are restrictions on its distribution, but these restrictions are designed to permit everything that a good cooperating citizen would want to do. What is not allowed is to try to prevent others from further sharing any version of GNU Emacs that they might get from you.²⁷⁹

In parallel with their technical development work, Stallman and the Free Software Foundation continued to further develop and refine the concept of copyleft and the terms and conditions of free software licenses and, “by 1989, [they] had crafted a clear legal framework for free software” in the form of the GNU General Public License (the GPL).²⁸⁰ The GPL was a more formal software license with its precise use of legal terminology and language, but, at its core, it still had the same radical copyleft licensing terms and provisions that guaranteed the four software freedoms.²⁸¹

What makes the concept of copyleft and its implementation in the GPL so remarkable was that free software developers had to apply their combined knowledge and mastery of social norms, technical code and legal rules in an unusual and non-conformist way to produce an innovative and surprising result – that is, to make software free and open through the creative use of the very same rules of normally restrictive copyright law, and preserve vital rights and freedoms under legally binding and enforceable contracts.²⁸² Copyleft was a great “hack” since it deftly exhibited the key elements of innovation, simplicity, mastery and non-conformity. Whereas copyright would ordinarily declare “all rights reserved”,²⁸³ copyleft went the opposite direction and, in a subversive yet playful way, made “all rights reversed”. In describing the GPL as a hack, Coleman states:

Stallman approached the law much like a hacker treats technol-

²⁷⁹ GNU Emacs General Public License.

²⁸⁰ E. Gabriella Coleman, *Coding Freedom* 69; see also Sam Williams, “Free As In Freedom” 109.

²⁸¹ “GNU General Public License version 1”; E. Gabriella Coleman, *Coding Freedom* 70; Gabriella Coleman, “Code is speech” 424.

²⁸² See E. Gabriella Coleman, *Coding Freedom* 70 and 88.

²⁸³ Richard Stallman, “The GNU Project” 23; see also E. Gabriella Coleman, *Coding Freedom* 70.

²⁸⁴ E. Gabriella Coleman, *Coding Freedom* 69-70.

ogy: as a system that by virtue of being systematic and logical, is hackable. In other words, he relied on the hacker technical tactic of clever reuse to imaginatively hack the law by creating the GNU GPL, a near inversion of copyright law.²⁸⁴

But the GPL is more than a software license since it has been “commonly referred to as the ‘Constitution’ of free software”.²⁸⁵ In a way, it also serves as a code of ethics and a manifesto for and about hacker culture since it expresses and enacts hacker norms and values.²⁸⁶ As Coleman explains, “Many hackers and developers learned about the ethical and legal message of free software early in its history, via the GPL or the ‘GNU Manifesto,’ both of which circulated on Usenet message boards and often accompanied pieces of free software”.²⁸⁷ What is astounding about the GPL was that “Stallman had done more than close up the escape hatch that permitted proprietary offshoots. He had expressed the hacker ethic in a manner understandable to both lawyer and hacker alike”.²⁸⁸ Copyleft as expressed in the GPL was a profound socio-techno-legal hack.²⁸⁹

As hacks go, the GPL stands as one of Stallman’s best. It created a system of communal ownership within the normally proprietary confines of copyright law. More importantly, it demonstrated the intellectual similarity between legal code and software code. Implicit within the GPL’s preamble was a profound message: instead of viewing copyright law with suspicion, hackers should view it as yet another system begging to be hacked.²⁹⁰

While Stallman and the Free Software Foundation made considerable advances in the 1980s in developing and advocating free software, it was the creation of the Linux operating system that would

²⁸⁵ E. Gabriella Coleman, *Coding Freedom* 76.

²⁸⁶ Sam Williams, “Free As In Freedom” 108 and 110; Tim Jordan, *Hacking* 63.

²⁸⁷ E. Gabriella Coleman, *Coding Freedom* 70.

²⁸⁸ Sam Williams, “Free As In Freedom” 109.

²⁸⁹ See Michael Dizon, “Rules of a networked society” 95; see Christopher Kelty, “Culture’s Open Sources” 502.

²⁹⁰ Sam Williams, “Free As In Freedom” 110.

²⁹¹ Sam Williams, “Free As In Freedom” 116 and 118; Richard Stallman, “The GNU Project” 28; E. Gabriella Coleman, *Coding Freedom* 76; Tim Jordan, *Hacking* 64-65.

ultimately give rise to a world-changing, global movement.²⁹¹

2.2.4.3 Linux

The goal of the GNU Project to create a free Unix-compatible operating system became a reality, when in the early 1990s, Linus Torvalds, then a student in Finland, created a “kernel”²⁹² and integrated existing GNU tools and components into it to produce Linux, an operating system that was licensed as free software under the GPL.²⁹³ Since Linux was developed to work on ubiquitous PC architecture, ordinary users could run an elegant and powerful operating system on their desktop computers.²⁹⁴

In addition to being “a fully functional operating system composed entirely of free software”,²⁹⁵ what made Linux especially amazing was that it was developed and maintained by Torvalds and an online community of thousands of volunteer programmers located in various parts of the world.²⁹⁶ According to Raymond, “the most important feature of Linux... was not technological but sociological”.²⁹⁷ Through the use of mailing lists, File Transfer Protocol (FTP) servers and other internet-based technologies, Linux and other free software developers could work collaboratively regardless of the physical and temporal distances between them.²⁹⁸ These online developer communities “do not tend to rely on any single one of the three bases

²⁹² “Kernel”, Computer Desktop Encyclopedia (which is described as “The nucleus of an operating system. It is the closest part to the machine level and may activate the hardware directly or interface to another software layer that drives the hardware. The kernel orchestrates the entire operation of the computer by slicing time for each system function and each application as well as managing all the computer’s resources. It typically resides in memory at all times”).

²⁹³ Sam Williams, “Free As In Freedom” 120-121; Richard Stallman, “The GNU Project” 28; E. Gabriella Coleman, Coding Freedom 74; Eric Raymond, The Cathedral and the Bazaar 15; Linus Torvalds and David Diamond, Just for Fun 59, 84, 96 and 163.

²⁹⁴ Eric Raymond, The Cathedral and the Bazaar 15; Sam Williams, “Free As In Freedom” 121; Linus Torvalds and David Diamond, Just for Fun 54-56 (who explain the elegance and power of Unix); Bruce Sterling, The Hacker Crackdown 107.

²⁹⁵ Sam Williams, “Free As In Freedom” 121.

²⁹⁶ E. Gabriella Coleman, Coding Freedom 75; Eric Raymond, The Cathedral and the Bazaar 16 and 21; Tim Jordan, Hacking 43; Margaret Elliot and Walt Scacchi, “Mobilization of software developers” 20.

²⁹⁷ Eric Raymond, The Cathedral and the Bazaar 16.

²⁹⁸ E. Gabriella Coleman, Coding Freedom 75-76; Eric Raymond, The Cathedral and the Bazaar 21; Tim Jordan, Hacking 49; Margaret Elliot and Walt Scacchi, “Mobilization of software developers” 17.

²⁹⁹ Siobhan O’Mahony and Fabrizio Ferraro, “The Emergence of Governance in an Open Source Community” 8, 11, 22 and 25.

of authority theorized by Weber (tradition, law, or charisma)”, and are often self-organized, have limited bureaucracies, and whose governance processes are based on consensus and meritocracy.²⁹⁹ As normally physically isolated hackers found kindred spirits online, they established and spread hacker culture across the global network of networks. According to Coleman, on the internet,

free software grew into a much larger technical and social movement in which geeks all over the world participated in the day-to-day development of free software.... This brought hackers’ long-standing ideals and practices for collaborating to unforeseen heights, and accidentally shifted where and how hacking could occur”.³⁰⁰

The online, collaborative and distributed development process and organizational model popularized by Linux “represent[ed] a relatively new approach to the development of complex software systems. Software development techniques used in [FOSS] projects are informal and self-managed with decisions generally made by meritocracy”.³⁰¹ Linux was the “world’s largest collaborative project”³⁰² and “demonstrated the feasibility of a large-scale, online collaboration effort where developers and users can be one and the same”.³⁰³ Linux was a clear refutation of Gates’s claim in his letter to computer hobbyists that the free sharing of software prevented complex and quality software from being written.³⁰⁴ In fact the “speed, reliability and efficiency” of the Linux development model equaled if not surpassed those of large software companies that made of closed and proprietary software.³⁰⁵ Coleman explains the impact that “this new era of networked hacking” that free software and the open internet engendered:

³⁰⁰ E. Gabriella Coleman, *Coding Freedom* 88.

³⁰¹ Margaret Elliot and Walt Scacchi, “Mobilization of software developers” 15.

³⁰² Linus Torvalds and David Diamond, *Just for Fun* 122.

³⁰³ Gwendolyn Lee and Robert Cole, “The Case of the Linux Kernel Development” 636.

³⁰⁴ See Bill Gates, “Open Letter to Hobbyists”; Tim Jordan, *Hacking* 43-44; Linus Torvalds and David Diamond, *Just for Fun* 227.

³⁰⁵ Gwendolyn Lee and Robert Cole, “The Case of the Linux Kernel Development” 636; see also Eric Raymond, *The Cathedral and the Bazaar* 21 and 33; see also E. Gabriella Coleman, *Coding Freedom* 76-77.

Linux initiated a global network of associations composed of hackers who, over time, came to not only identify and alter the principles of freedom first enshrined by Stallman but also shift the material practice of collaborative hacking. The pragmatic and ethical hallmarks of hacking – innovation, creativity, collaboration, a commitment to openness, and imaginative problem-solving – that Stallman established as a bulwark against proprietization became the basis of long-distance free software development.³⁰⁶

These online software development communities performed many acts of hacking: they created computer programs and distributed them under copyright licenses that ensured that anyone was free to learn, explore, modify and share the underlying source code; they intentionally broke and subverted the legal regime of intellectual property rights to preserve and protect the freedom and openness of their creations; and they believed that the free and open model to software development produced programs that were more robust and secure. Hackers were not only making free software available to everyone, but they were gaining supporters and adherents on massive and global scale online and offline.³⁰⁷

2.2.4.4 FOSS and other movements

Recognizing the revolutionary potential of the online, community-based model to software development,³⁰⁸ Linux and other free software were rebranded as “open source” beginning in the late 1990s.³⁰⁹ The shift of the nomenclature from “free” to “open source” was intended to distance Linux from the allegedly ideological undertones of “free software” and make it more appealing to enterprises and businesses.³¹⁰ Open source sought to emphasize Linux’s techni-

³⁰⁶ E. Gabriella Coleman, *Coding Freedom* 75.

³⁰⁷ Linus Torvalds and David Diamond, *Just for Fun* 122.

³⁰⁸ Gwendolyn Lee and Robert Cole, “The Case of the Linux Kernel Development” 642.

³⁰⁹ Eric Raymond, *The Cathedral and the Bazaar* 175.

³¹⁰ Eric Raymond, *The Cathedral and the Bazaar* 175-176; Linus Torvalds and David Diamond, *Just for Fun* 164 and 166-167.

³¹¹ Eric Raymond, *The Cathedral and the Bazaar* 21 and 175-177; see also Josh Lerner and Jean Tirole, “The Economics of Technology Sharing”.

cal (rather than moral or ethical) advantages over software developed using the hierarchical, top-down “Cathedral” method.³¹² The aim was to make choosing open source a pragmatic as opposed to a political decision.³¹² While there is a long-running debate about the difference between “free” versus “open source” software,³¹³ since scholars consider the schism a theoretical rather than practical matter,³¹⁴ I collectively refer to computer programs produced and licensed pursuant to the hacker ideals of free sharing and open collaboration as “free and open source software” (or FOSS for short).³¹⁵ Aside from Linux, Apache (web server), MySQL (database), Python (programming language), WebKit (browser rendering engine), Drupal (content management system), and Android (mobile operating system) are a few of the many examples of FOSS that are extremely popular among developers and users alike.³¹⁶ There are likewise many developers and commercial companies whose activities and businesses are built on FOSS and the FOSS development model. Technology companies such as IBM, Oracle, Apple and Google contribute to FOSS projects.

The triumph of FOSS and its accompanying techno-social movement is all the more extraordinary when one considers that FOSS emerged during a period when the scope and degree of protection and enforcement of intellectual property rights were possibly at their most severe.³¹⁷ As Coleman explains, FOSS prospered remarkably “during an era of such unprecedented transformations in intellectual property law that critics have described it in ominous terms like ‘information feudalism’. Never before has a single legal regime of copyrights and patents reigned supreme across the globe.”³¹⁸ FOSS funda-

³¹² Eric Raymond, *The Cathedral and the Bazaar* 175.

³¹³ Richard Stallman, “Why Open Source misses the point of Free Software”; David Berry, “The Contestation of Code”.

³¹⁴ Brian Alleyne, “We are all hackers now” 20; Christopher Kely, *Two Bits* 14

³¹⁵ See “The Free Software Definition”; see “The Open Source Definition” (for precise definitions of what are considered FOSS).

³¹⁶ See Michael Dizon, “Rules of a networked society” 94-95.

³¹⁷ E. Gabriella Coleman, *Coding Freedom* 62 and 72.

³¹⁸ E. Gabriella Coleman, *Coding Freedom* 62.

³¹⁹ E. Gabriella Coleman, *Coding Freedom* 72.

mentally changed the principles and practices of the software industry despite the adoption of treaties such as the Trade-Related Aspects of Intellectual Property Rights (TRIPs) and the WIPO Internet Treaties.³¹⁹ Part of the reason why FOSS was impervious and invisible to law was because, through the use of copyleft licenses, FOSS developers were working within the legal order and according to the letter of the law (although FOSS was ultimately subverting the system by playing on the latter's internal inconsistencies, gaps and conflicts).³²⁰ Another reason why FOSS flew under the radar was because most everyone, including legislators, law enforcement and software companies were either oblivious to FOSS or considered it trivial and inconsequential.³²¹ Of course, in the 2000s after FOSS had made great headway to become a formidable force in the technology sphere, the SCO Group filed a number of unsuccessful cases against prominent companies that used and developed Linux,³²² and, in addition to spreading fear, uncertainty and doubt about FOSS, the software giant Microsoft started to demand licensing fees from companies using Linux on the ground that the latter was infringing some of its patents.³²³ So, despite their keen appreciation and expertise in the vagaries of copyright and other intellectual property laws, FOSS developers were not fully immune to the influence of law.³²⁴

On a deeper level, FOSS and the FOSS movement are socially and culturally significant because they helped spread the hacker mentality and ideals beyond software and hacking. Their underlying “open anything”³²⁵ philosophy has inspired similar movements, causes and campaigns across wide-ranging, non-technical domains – from aca-

³²⁰ E. Gabriella Coleman, *Coding Freedom* 73; see Andrew Feenberg, “Escaping the Iron Cage, or, Subversive Rationalization and Democratic Theory”.

³²¹ E. Gabriella Coleman, *Coding Freedom* 69-70; Sam Williams, “Free As In Freedom” 91.

³²² See *SCO Group v. International Business Machines, Inc.*

³²³ Margaret Elliot and Walt Scacchi, “Mobilization of software developers” 22-23; Linus Torvalds and David Diamond, *Just for Fun* 167.

³²⁴ See Gabriella Coleman, “Code is Speech”.

³²⁵ Linus Torvalds and David Diamond, *Just for Fun* 232 and 234.

demic publishing to education initiatives and to new modes of governance.³²⁶ Open Access,³²⁷ Creative Commons,³²⁸ Access to Knowledge,³²⁹ Open Science,³³⁰ Open Government,³³¹ and Open Data³³² are some of the noteworthy causes and initiatives that draw from or have been sparked by FOSS.

2.2.5 OF THE WORLD WIDE WEB OF COMPUTERS AND COMMUNITIES – HACKTIVISTS

2.2.5.1 Hacklabs, hackmeets and hacker cons

In the same way that the wider use and development of the internet and the World Wide Web (the Web) in the 1990s provided a technological base that allowed online FOSS developer communities to flourish, global computing and communications networks, coupled with the cross-cutting forces associated with globalization, profoundly affected hackers in two main ways: their greater socialization and politicization; and the broader dissemination and use of hacking technologies by hackers and non-hackers alike for socio-political purposes, causes and campaigns.³³³ The development and expansion of socio-technical networks of people and technologies paved the way for the cross-fertilization between hackers (specifically their values and tools) and other groups and subcultures such as activists, anarchists and artists.³³⁴ The global network of networks had a noticeable impact on radical groups and alternative movements: “The Internet amplifies, accelerates, and, in some ways, transforms communication with-

³²⁶ Lawrence Lessig, Code: version 2 199.

³²⁷ UK Open Access Implementation Group, “The Case for Open Access”;

³²⁸ Creative Commons; see Lawrence Lessig, Code: version 2 199; but see Niva Elkin-Koren, “Exploring Creative Commons”.

³²⁹ Access to Knowledge, <<http://www.cptech.org/a2k/>> accessed 12 August 2013

³³⁰ The OpenScience Project, <<http://www.openscience.org/blog/>> accessed 12 August 2013

³³¹ Open Government Initiative, <<http://www.whitehouse.gov/open>> accessed 12 August 2013<<http://www.whitehouse.gov/open>> accessed 12 August 2013.

³³² Open Data Commons <<http://opendatacommons.org/>> accessed 12 August 2013; “Open Data Sites”, <<http://www.data.gov/opendatasites>> accessed 12 August 2013.

³³³ Tim Jordan, Activism! 14; Paul Taylor, “From hackers to hacktivists” 637; Maxigas, “Hacklabs and hackerspaces” 2; see Lauren Langman, “A Critical Theory of Internetworked Social Movements” 51 (for the consequences of globalization).

³³⁴ Paul Taylor, “From hackers to hacktivists” 637; Tim Jordan, Activism! 19, 23 and 127.

in a group's internal organization, but it also changes the relationship between one group or movement's network and those of its potential competitors or collaborators".³³⁵ The internet brought about internal and external changes in social groups and movements that made them both inwardly and outwardly focused.³³⁶

Technical networks made it possible for hackers to form social connections with other groups. According to Taylor, the "use of the world wide web [w]as an integral part of new social movements" as "electronic culture facilitate[d] the emergence of global groups of like-minded radicals".³³⁷ Hacktivism thus came about due to the interfacing and interactions between hacker culture and other activist and alternative traditions.³³⁸ It is worth pointing out that the Electronic Frontier Foundation (EFF), a prominent US digital rights organization, was started in 1990 as a direct result of the legal crackdowns against underground hackers and the perceived need to protect people's digital and civil freedoms.³³⁹ As such, in contrast to early hacker generations, the activities of hacktivists do not remain solely within the technical realm but draw upon and bring to bear a combination of hacker, activist or artistic beliefs and praxis. The Critical Art Ensemble (CAE) and the Electronic Disturbance Theatre (EDT), which were formed in the mid-1990s, are well-known examples of hybrid associations and activities that hacktivists take part in.³⁴⁰ The CAE is noteworthy for being the group that issued a formal call "for the development of electronic civil disobedience and the politicization of hackers".³⁴¹ Fusing hacking, media and art as a form of "culture jamming",

³³⁵ Andrew Chadwick, *Internet Politics* 118; Lauren Langman, "A Critical Theory of Internetnetworked Social Movements" 58-60.

³³⁶ Andrew Chanwick, *Internet Politics* 118; Paul Taylor, "From hackers to hacktivists" 630; Maxigas, "Hacklabs and hackerspaces" 2; Stefania Milan and Arne Hintz, "Dynamics of Cyberactivism" 1.

³³⁷ Paul Taylor, "From hackers to hacktivists" 637-638.

³³⁸ See Stefania Milan and Arne Hintz, "Dynamics of Cyberactivism"; see Martina Gillen, "Is there still a future for online protest in the Anonymous world?" 5.

³³⁹ Bruce Sterling, *The Hacker Crackdown* 12; Maxigas, "Hacklabs and hackerspaces" 5.

³⁴⁰ Tim Jordan, *Activism!* 120-121; Maxigas, "Hacklabs and hackerspaces" 2-3; Jordan, *Hacking* 71-72.

³⁴¹ Critical Art Ensemble, *Electronic Civil Disobedience* 7; see also Tim Jordan, *Activism!* 120; see also Andrew Chadwick, "Internet Politics" 132; see also Tatiana Bazzichelli, *Networking: The Net as Artwork* 173; see also Paul Taylor, "Editorial: Hacktivism" 5; see also Giovanni Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age* 6.

the CAE “brought to fore issues of access frequency regulation, popular education, editorial policies and mass creativity, all of which pointed in the direction of lowering the barriers of participation for cultural and technological production”.³⁴² The EDT, for its part, famously utilized a computer program called Tactical FloodNet to disrupt government websites in support of the Zapatista uprising in Mexico.³⁴³

In addition to these hybrid groups and campaigns, the merging of hacker and alternative cultures manifested itself as well in physical spaces and social gatherings – hacklabs and other hacker events. According to Yuill,

Hacklabs are voluntarily run spaces providing free public access to computers and the internet. They generally make use of reclaimed and recycled machines running GNU/Linux and, alongside providing computer access, most hacklabs run workshops in a range of topics from basic computer use and installing GNU/Linux software, to programming, electronics, and independent (or pirate) radio broadcast.³⁴⁴

While hacklabs closely resemble makers’ hackerspaces and they are often used synonymously, they differ in a number of ways.³⁴⁵ For one, they are based on distinct histories and ideologies.³⁴⁶ Unlike hackerspaces, which are located in leased premises, hacklabs were situated in squatted buildings or part of community centers and media labs.³⁴⁷ While hackerspaces can trace their lineage to the Chaos Computer Club and its clubroom and eventual headquarters,³⁴⁸ hacklabs were part of the anarchist squats and autonomist social centers.³⁴⁹ They therefore drew from the broader anarchist and au-

³⁴² Maxigas, “Hacklabs and hackerspaces” 3.

³⁴³ Tim Jordan, *Activism!* 121; Andrew Chandwick, “Internet Politics” 131-132; Tatiana Bazzichelli, *Networking: The Net as Artwork* 173 (the Tactical FloodNet code, like other hacktivist tools, is released under a FOSS licence); Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”; Lauren Langman, “A Critical Theory of Internetworked Social Movements” 71.

³⁴⁴ Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”.

³⁴⁵ Maxigas, “Hacklabs and hackerspaces” 1.

³⁴⁶ Maxigas, “Hacklabs and hackerspaces” 1.

³⁴⁷ Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”; Maxigas, “Hacklabs and hackerspaces” 1-2.

³⁴⁸ Maxigas, “Hacklabs and hackerspaces 4; Hackerspaces – The Beginning 6-7.

³⁴⁹ Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”; Maxigas, “Hacklabs and hackerspaces” 1; Johannes Grenz-further and Frank Apunkt Schneider, “Rewriting Hacking the Spaces”.

onomous movements and “grew out of the needs and aspirations of squatters and media activists”.³⁵⁰ They also had close connections with alter-globalization and other radical, transnational causes.³⁵¹ As such, hacklabs were not just workshops but social centers that “would provide space for initiatives that sought to establish an alternative to official institutions”.³⁵² Hacklabs were places to learn about or work on “free software development, security and anonymity, electronic art and media production”.³⁵³

In addition to hacklabs, hacktivists gathered with other alternative groups in various conferences, camps and events.³⁵⁴ The greater impetus and value placed on socialization led to more “networking, collective meetings and sharing experiences” by hackers.³⁵⁵ The Chaos Computer Club and the hacker magazines Phrack and 2600 have organized regular hacker “cons” (short for conferences) in Europe and the United States that bring together different types of hackers and activists.³⁵⁶ Organized by Italian hacktivists, hackmeetings or hackmeets are “temporary gathering of hackers and hacktivists in which skills, tools and knowledge are exchanged and projects developed”.³⁵⁷ Hackmeets involved “sharing collective information and knowledge about everything that concerns technology, from the computer to the radio, to video, to artistic experimentation”.³⁵⁸ Outdoor hacker camps were popularized by hacktivists in the Netherlands.³⁵⁹ Hacker events evince how hacking is intimately a “networking practice”.³⁶⁰ In these physical

³⁵⁰ Maxigas, “Hacklabs and hackerspaces” 1-3; see also Johannes Grenzfurthner and Frank Apunkt Schneider, “Rewriting Hacking the Spaces”.

³⁵¹ Maxigas, “Hacklabs and hackerspaces” 4.

³⁵² Maxigas, “Hacklabs and hackerspaces” 2; see also Johannes Grenzfurthner and Frank Apunkt Schneider, “Rewriting Hacking the Spaces”; see also Tatiana Bazzichelli, *Networking: The Net as Artwork* 166.

³⁵³ Maxigas, “Hacklabs and hackerspaces” 4.

³⁵⁴ Maxigas, “Hacklabs and hackerspaces” 5; Peter Ludlow, “Wikileaks and Hacktivist Culture” 25-26.

³⁵⁵ Tatiana Bazzichelli, *Networking: The Net as Artwork* 141.

³⁵⁶ Hackerspaces - The Beginning 7; Maxigas, “Hacklabs and hackerspaces” 5; Shmeck, “25 Years of SummerCon”; see Gabriella Coleman, “The Hacker Conference” 49.

³⁵⁷ Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”; see also Maxigas, “Hacklabs and hackerspaces” 3; see also Tatiana Bazzichelli, *Networking: The Net as Artwork* 163-164.

³⁵⁸ Tatiana Bazzichelli, *Networking: The Net as Artwork* 164.

³⁵⁹ Maxigas, “Hacklabs and hackerspaces” 5; Tatiana Bazzichelli, *Networking: The Net as Artwork* 143.

³⁶⁰ Tatiana Bazzichelli, *Networking: The Net as Artwork* 139.

and temporal spaces, hacktivists, activists and artists come together to work on, among other things, art projects, free software and recycled hardware.³⁶¹ In this way, “physical and virtual spaces [are] enmeshed due to the activists’ use of electronic media communications” to connect with various socio-technical networks.³⁶²

2.2.5.2 Taking to the streets and the information superhighways

Hactivists engage in overtly “politically motivated hacking” and “[draw] upon the resources of the hacker community and hacker culture”.³⁶³ The emergence of hacktivists should come as no surprise since hacking is inherently a political act.³⁶⁴ From the very beginning, hacking “has often been combined with broad social and political goals”.³⁶⁵ The values and behaviors of the original hackers at MIT had a strong anti-establishment streak and countercultural dimension. These non-conformist attitudes and approaches to technology, law and authorities are similarly shared and carried out by the succeeding generations of hackers.³⁶⁶ Hacking has a highly politicized and subversive nature since the “distinguishing feature of hacking resides in its ingenious reinterpretation and re-engineering of the systems that it confronts”.³⁶⁷ However, unlike the MIT hackers, hacktivists do not view computers and other technologies as ends in themselves, but as critical means to achieve certain higher goals for the benefit of others and society.³⁶⁸ While freedom of access and the openness of technologies continue to be important concerns, hacktivists have transcended the primary concerns of previous hacker generations and engage

³⁶¹ Maxigas, “Hacklabs and hackerspaces” 4; Simon Yuill, “All Problems of Notation Will Be Solved by the Masses”.

³⁶² Maxigas, “Hacklabs and hackerspaces” 3.

³⁶³ Andrew Chadwick, “Internet Politics” 129-131; see also Tim Jordan, *Activism!* 119; see also Paul Taylor, “From hackers to hacktivists” 629; see also Tim Jordan, *Hacking* 96.

³⁶⁴ Gabriella Coleman, “Hacker politics and publics” 516; Brian Alleyne, “We are all hackers now” 24; Paul Taylor, “From hackers to hacktivists” 629.

³⁶⁵ Andrew Chadwick, *Internet Politics* 131; see also Lauren Langman, “A Critical Theory of Interneted Social Movements” 63.

³⁶⁶ Paul Taylor, “From hackers to hacktivists” 644.

³⁶⁷ Paul Taylor, “From hackers to hacktivists” 633.

³⁶⁸ Paul Taylor, “From hackers to hacktivists” 630; Peter Ludlow, “Wikileaks and Hactivist Culture” 26.

with issues that go beyond purely technical matters and require social commitment and political action in the physical world.³⁶⁹ Taylor notes, “traditional political militancy allied to a new level of technology savvy has resolved the within/without dilemma that hackers generally avoided”.³⁷⁰ In this sense, hacktivists share an affinity with underground hackers who also engaged in techno-social hacking.³⁷¹ While members of the digital underground primarily used their technical knowledge and skills, the motivation of hacking for them was to produce socio-political change and have an impact on society.³⁷² As with underground hackers, hacktivists seek to “blend the social and the technical” and this requires bringing their cause and taking action in both real and virtual spaces.³⁷³

Unlike other hacker types who are generally content with making an impact on the world exclusively through technology, hacktivists want to directly engage with and change the technological society itself whether through technical or non-technical means and action. For hacktivists, “hacking and making social changes” occur “simultaneously, one in and of the other”.³⁷⁴ They desire to go beyond “hacking’s over-identification with its tools” and use “techniques which can blend both technical methods and political aims”.³⁷⁵ As Jordan explains, “The rise of hacktivism has not superseded or destroyed hacker politics, but has reconfigured it within a broader political landscape”; that is, from “‘information politics’, traditionally the centre of hacker politics, [to] a broadening out into non-virtual politics”.³⁷⁶

This expansion and outward orientation means that hacktivists fight for their causes with their keyboards and their feet, on the so-

³⁶⁹ Tim Jordan, *Activism!* 121; Paul Taylor, “From hackers to hacktivists” 630.

³⁷⁰ Paul Taylor, “From hackers to hacktivists” 637.

³⁷¹ Tatiana Bazzichelli, *Networking: The Net as Artwork* 139; Andrew Chandwick, “Internet Politics” 133 (US underground hackers Cult of the Dead Cow also took part in hacktivism); Tim Jordan, *Activism!* 127-128 (who explains Cult of the Dead Cow’s hacktivism).

³⁷² Tatiana Bazzichelli, *Networking: The Net as Artwork* 140.

³⁷³ Paul Taylor, “From hackers to hacktivists” 636.

³⁷⁴ Jordan, *Hacking* 97.

³⁷⁵ Paul Taylor, “From hackers to hacktivists” 634 and 641.

³⁷⁶ Tim Jordan, *Activism!* 121.

called information superhighways and in the streets.³⁷⁷ For example, during the activist mobilizations against the World Trade Organization (WTO) meeting in Seattle in 1999, “there were simultaneous online and offline protests. As demonstrators occupied the streets, hacktivists occupied websites”.³⁷⁸ The hacktivist group Anonymous similarly combined online hacking (e.g., conducting distributed denial of service (DDoS) attacks to impair access to the websites and online services of target government agencies and companies) with traditional forms of activism like holding public street protests and mass demonstrations.³⁷⁹ When hackers Jon Johansen and Dmitry Sklyarov were arrested and charged for violating the US Digital Millennium Copyright Act when they published information on how to circumvent copy protection mechanisms on DVDs and ebooks, many hackers mobilized, took to the streets and the Web, protested in new and creative ways (e.g., transforming the controversial circumvention code into a poem so it would be protected under freedom of speech), and were successful in getting charges against Sklyarov dropped.³⁸⁰

Hacktivism is considered a genuinely new form of socio-political mobilization because it “tactically combines the cyberspatial web and physical world”.³⁸¹ It involves many forms of hacking: hacktivists break or interrupt the functioning of computer systems as a form of protest and civil disobedience; they design and create technologies that protect and keep secure the identity of activists and dissidents; and they are very public about their campaigns and causes and they openly share their technical know-how and creations so everyone is free to explore and build on their technologies and learn about their experiences. The merging of online and offline action is uniquely

³⁷⁷ Tim Jordan, *Activism!* 126; Paul Taylor, “Editorial: Hacktivism” 7; Reid Skibell, “Cybercrimes & Misdemeanors” 938.

³⁷⁸ Tim Jordan, *Activism!* 122; see also Lauren Langman, “A Critical Theory of Interneted Social Movements” 68.

³⁷⁹ E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”; Martina Gillen, “Is there still a future for online protest in the Anonymous world?” 5; Stefania Milan and Arne Hintz, “Dynamics of Cyberactivism” 9.

³⁸⁰ Gabriella Coleman, “Code is Speech” 435, 437, 441, 444, 446 and 447.

³⁸¹ Paul Taylor, “From hackers to hacktivists” 640 and 644; see also Andrew Chadwick, *Internet Politics* 115.

suiting for transforming a world that is dependent on and governed by technology.³⁸² As Taylor states, due to “the ever-more closely imbricated nature of the technological and the social, [hacking] promises more radical results if successfully carried out. Each technical act of reversal promises to contain a more politically charged and symbolic payload”.³⁸³ Despite the two fronts that hacktivists engage in, it is important to note that the line between the real and the virtual is not always clear and hacks can impinge on both domains. As Jordan explains, “First, many real-world institutions are affected by cyberspace. Computer networks control all sorts of real-world facilities.... Second, violence is not always physical, and damage to emotions and selves can occur in virtual lands”.³⁸⁴ In this way, hacktivists can change and reshape both tangible and intangible realities.

2.2.6 OF OPEN TECHNOLOGIES, PROJECTS AND SPACES – MAKERS

2.2.6.1 Open innovation

Makers share many things in common with previous hacker generations, especially computer hobbyists and FOSS developers. Makers primarily hack pursuant to the hacker tradition of freedom and openness.³⁸⁵ However, makers are interested in all kinds of technologies and not only those relating to computing and communications.³⁸⁶ They aspire for open innovation, i.e., to open everything and create anything.³⁸⁷ Makers are involved in diverse projects such as “free software development, computer recycling, wireless mesh networking, microelectronics, open hardware, 3D printing, machine work-

³⁸² Lauren Langman, “A Critical Theory of Internetworked Social Movements” 53-54; Noah Hampson, “Hacktivism” 517 and 536.

³⁸³ Paul Taylor, “From hackers to hacktivists” 644.

³⁸⁴ Tim Jordan, *Activism!* 126.

³⁸⁵ Travis Good, “What is ‘Making?’”.

³⁸⁶ IKEA hackers <<http://www.ikeahackers.net/>> accessed 16 August 2013; Andrew Schrok, “What Keeps Hacker and Maker Spaces Going?”; Peter Troxler, “Libraries of the Peer Production Era”.

³⁸⁷ Chris Anderson, *Makers* 94; Bre Pettis, “Open Source Ethics and Dead End Derivatives”.

shops and cooking”.³⁸⁸ They engage in various forms of hacking: they are not worried about voiding warranties and they freely break and take apart electronic devices in order to explore the insides of these black boxes, learn how they work and make them perform in new, surprising and creative ways; and they are very open about their activities and they make available and share information about their projects online. Even though their attention has expanded and gone beyond computers, they still adhere to the “hands-on imperative” espoused by the original MIT hackers that the best way to learn and create is through actual doing.³⁸⁹ Like the computer hobbyists, they are community-oriented and they are adept at working on both hardware and software projects.³⁹⁰ Continuing the work of FOSS developers, makers are trying to ensure that hardware is as accessible and generative as FOSS by developing appropriate licenses under which their creations can be freely distributed to and used by the public.³⁹¹ Despite the difficulty of exactly transposing copyleft to the physical realm of hardware,³⁹² this has not prevented makers from creating and building open technologies and platforms. For makers, “open source means open everything: electronics, software, physical design, documentation, even the logo”.³⁹³

The worldwide maker community has produced and given rise to many products, services, communities and organizations that promote the idea of open innovation for commercial and non-commercial purposes. The RepRap project is a popular, low-cost and open source 3D printer that was created and developed by an online community of makers.³⁹⁴ Drawing from the FOSS movement, “all of the designs produced by the project are released under a free software

³⁸⁸ Maxigas, “Hacklabs and hackerspaces 5.

³⁸⁹ Steven Levy, *Hackers* 28; see also Andrew Schrok, “What Keeps Hacker and Maker Spaces Going?”.

³⁹⁰ Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”.

³⁹¹ Open Source Hardware Association, “Open Source Hardware (OSHW) Statement of Principles 1.0”; Chris Anderson, *Makers* 19.

³⁹² Andrew Katz, “Towards a Functional Licence for Open Hardware”; Walter, “The Makerbot/Thingiverse move to the Dark Side”.

³⁹³ Chris Anderson, *Makers* 94.

³⁹⁴ RepRap; Chris Anderson, *Makers* 20.

license, the GNU General Public License”.³⁹⁵ The electronics of the RepRap 3D printer are built on Arduino,³⁹⁶ which is “an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board”.³⁹⁷ A microcontroller is “a single chip that contains the processor (the CPU), non-volatile memory for the program (ROM or flash), volatile memory for input and output (RAM), a clock and an I/O control unit”.³⁹⁸ It is literally “a computer on a chip” and its basic architecture closely resembles the main components of PCs such as the Altair and the Apple II.³⁹⁹ The Arduino hardware, software and documentation are made publicly available through creative commons and other FOSS licenses.⁴⁰⁰ For example, “all of the original design files (Eagle CAD) for the Arduino hardware” are released “under a Creative Commons Attribution Share-Alike license, which allows for both personal and commercial derivative works, as long as they credit Arduino and release their designs under the same license”.⁴⁰¹ Many makers use Arduino microcontroller boards to act as the brains of their projects,⁴⁰² and, like RepRap, a worldwide community of developers and users contribute to and support Arduino.⁴⁰³

Makers believe in the importance of free sharing and open collaboration so most projects are made available and worked on together online.⁴⁰⁴ Like FOSS developers, makers have made full and extensive use of the internet to connect, communicate, and collaborate on projects.⁴⁰⁵ Reminiscent of computer hobbyists, makers “show off”

³⁹⁵ RepRap Project.

³⁹⁶ RepRap Project.

³⁹⁷ “What is Arduino?”.

³⁹⁸ “Microcontroller”, Computer Desktop Encyclopedia.

³⁹⁹ “Microcontroller”, Computer Desktop Encyclopedia.

⁴⁰⁰ “What is Arduino?”; “Frequently Asked Questions”, Arduino.

⁴⁰¹ “Frequently Asked Questions”, Arduino.

⁴⁰² “Arduino Projects”, Instructables; “Things tagged with ‘arduino’”, MakerBot Thingiverse; Maxigas, “Hacklabs and hackerspaces 6.

⁴⁰³ Arduino, <<http://www.arduino.cc/>> accessed 30 August 2013; but see Massimo Banzi, “Fighting for Arduino” <<http://makezine.com/2015/03/19/massimo-banzi-fighting-for-arduino/>> accessed 5 February 2016 (about the falling out between Arduino’s core developers over intellectual property and commercial issues).

⁴⁰⁴ Chris Anderson, *Makers 21*; see Instructables; see MakerBot Thingiverse.

⁴⁰⁵ Travis Good, “What is ‘Making’?”; Ken Denmead, “Why the Maker Movement is Here to Stay”.

⁴⁰⁶ Ken Denmead, “Why the Maker Movement is Here to Stay”; Peter Troxler, “Libraries of the Peer Production Era”.

their creations in both physical and virtual spaces for peer recognition and to get feedback from the community.⁴⁰⁶ There are indeed significant parallels between makers and computer hobbyists. In the same way that the PC started as a hobbyist project in the Homebrew Computer Club, makers are developing low-cost 3D printers and other disruptive technologies in hackerspaces.⁴⁰⁷ Makers and people writing about the maker movement are convinced that low-cost 3D printers have the potential to be as world-changing as the PC was, and they will lead to a digital manufacturing revolution.⁴⁰⁸

2.2.6.2 Hackerspaces

In addition to the open technologies and innovative projects that they are building, makers are especially distinct from other hacker types with regard to where they hack – hackerspaces. Hackerspaces have their origins in Europe and the United States in the 1990s.⁴⁰⁹ However, they only became a global phenomenon and an international movement in the late 2000s as a result of the cross-fertilization between European and US hackers during events organized by the Chaos Computer Club in Germany in 2007 on how to develop and run “community-operated physical places, where people can meet and work on their projects”.⁴¹⁰ The tangible, visible and public nature of hackerspaces has proven to be very beneficial to makers since it has led to “community involvement” both internally within their groups and externally with the local communities they inhabit.⁴¹¹ Hackerspaces are physical sites where makers can “come and have meetings,

⁴⁰⁷ Chris Anderson, “The New MakerBot Replicator Might Just Change Your World”; Chris Anderson, *Makers* 22-23.

⁴⁰⁸ Chris Anderson, “The New MakerBot Replicator Might Just Change Your World”; Chris Anderson, *Makers* 102.

⁴⁰⁹ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”; Nick Farr, “Respect the Past, Examine the Present, Build the Future”.

⁴¹⁰ Hackerspaces.org <<http://hackerspaces.org/wiki/>> (for a definition of hackerspaces); see also Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”; see also Hackerspaces - The Beginning; see also John Borland, “‘Hacker space’ movement sought for U.S.”; see also Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”; see also Jens Ohlig and Lars Weiler, “Building a Hacker Space”; see also Andrew Schrok, “What Keeps Hacker and Maker Spaces Going?”; see also Chris Anderson, *Makers* 18; see also Maxigas, “Hacklabs and hackerspaces” 5.

⁴¹¹ John Borland, “‘Hacker space’ movement sought for U.S.”; see also Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”; see also Steven Kurutz, “One Big Workbench”.

do good works, and show the community what they're really about.... show people that hackers aren't criminals, that they're creative types who have a way of making technology do things [that were not expected or] it wasn't originally intended for".⁴¹² This is in stark contrast to the secrecy and mystery surrounding the underground hackers. In hackerspaces, makers "could be perfectly open about their work, organize officially, gain recognition from government and respect from the public by living and applying the [h]acker ethic in their efforts".⁴¹³

Hackerspaces are typically communally organized and run.⁴¹⁴ They "tend to be loosely organized, governed by consensus, and infused with an almost utopian spirit of cooperation and sharing".⁴¹⁵ In general, hackerspaces are designed and built according to a catalog of basic "design patterns", which were presented at the Chaos Communication Congress in Germany in 2007.⁴¹⁶ The design patterns were based on and inspired by existing or best practices of the German hackerspaces c-base and the Chaos Computer Club Cologne (C4), and are still considered "the best guiding theory behind the global [h]ackerspace [m]ovement".⁴¹⁷ The templates offer guidance on or solutions to the wide range of issues which members of hackerspaces face from establishment to day-to-day operation.⁴¹⁸ There are design patterns on sustainability, infrastructure, communications, interior design, membership and fees, meetings, recruitment, decision-making, and members' rights and responsibilities.⁴¹⁹ Membership rights normally include getting a key to the hackerspace, use of common equipment

⁴¹² John Borland, "Hacker space' movement sought for U.S."

⁴¹³ Nick Farr, "Respect the Past, Examine the Present, Build the Future"; see also Peter Troxler, "Libraries of the Peer Production Era".

⁴¹⁴ Dylan Tweney, "DIY Freaks Flock to 'Hacker Spaces' Worldwide"; Steven Kurutz, "One Big Workbench".

⁴¹⁵ Dylan Tweney, "DIY Freaks Flock to 'Hacker Spaces' Worldwide"; see also Steven Kurutz, "One Big Workbench"; see also Maxigas, "Hacklabs and hackerspaces" 6.

⁴¹⁶ Jens Ohlig and Lars Weiler, "Building a Hacker Space"; Dylan Tweney, "DIY Freaks Flock to 'Hacker Spaces' Worldwide".

⁴¹⁷ Nick Farr, "The Rights and Obligations of Hackerspace Members"; see also Jens Ohlig and Lars Weiler, "Building a Hacker Space"; see also Nick Farr, "The Rights and Obligations of Hackerspace Members"; see also Maxigas, "Hacklabs and hackerspaces 5; see also Hackerspaces - The Beginning 11.

⁴¹⁸ Jens Ohlig and Lars Weiler, "Building a Hacker Space".

⁴¹⁹ Jens Ohlig and Lars Weiler, "Building a Hacker Space".

⁴²⁰ Nick Farr, "The Rights and Obligations of Hackerspace Members"; see also Maxigas, "Hacklabs and hackerspaces 6.

and tools, and having a space to work on and store their projects.⁴²⁰ Following the design patterns, “[m]ost members pay dues to cover rent and expenses and share the obligation of administration, publicity, documentation, and other duties essential to keeping a space open and flourishing”.⁴²¹ A portion of the fees can go toward the purchase of equipment and tools.⁴²² Like the Homebrew Computer Club, there is a strong communitarian spirit within hackerspaces; “[m]ost of the space – and the tools – are shared by all members, with small spaces set aside for each member to store items and projects for their own use”.⁴²³ Aside from computers and communications equipment, hackerspaces are full of diverse tools such as “laser cutters, 3-D printers, miter saws and other woodworking tools, esoteric electronics like spectrophotometers and tiny single-chip computers known as micro-controllers”.⁴²⁴ Online group communications are carried out on or through mailing lists, wikis and Internet Relay Chat (IRC) channels.⁴²⁵

What is interesting about the communities and sites that form the hackerspace movement is that while they are steeped in their locality, they have a global orientation and outlook. Tweney explains, “Hacker spaces aren’t just growing up in isolation: They’re forming networks and linking up with one another in a decentralized, worldwide network” primarily through the website hackerspaces.org, which “collects information about current and emerging hackerspaces, and provides information about creating and managing new spaces”.⁴²⁶ In fact, becoming part of the global hackerspace community “is essentially a matter of self-declaration – an entry on the hackerspaces.org wiki is sufficient”.⁴²⁷ Through their engagement with their local commu-

⁴²¹ Nick Farr, “The Rights and Obligations of Hackerspace Members”; see also Steven Kurutz, “One Big Workbench”.

⁴²² Steven Kurutz, “One Big Workbench”; Peter Troxler, “Libraries of the Peer Production Era”.

⁴²³ Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”; see also Peter Troxler, “Libraries of the Peer Production Era”; see also Ken Denmead, “Why the Maker Movement is Here to Stay”.

⁴²⁴ Steven Kurutz, “One Big Workbench”.

⁴²⁶ Jens Ohlig and Lars Weiler, “Building a Hacker Space”; Maxigas, “Hacklabs and hackerspaces” 6.

⁴²⁷ Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”.

Peter Troxler, “Libraries of the Peer Production Era”; see also Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”.

nities, other hackerspaces and the world at large, makers are applying the hacker values of collaboration and sharing not just to their technical activities but to their social relations as well. Makers' openness to the outside world distinguishes them from previous generations of hackers who mainly lived out the hacker ethic exclusively within their groups.⁴²⁸ Among makers, there is an appreciation of the importance of social openness:

Becoming welcoming to the outside world helps ensure our collective success and sustainability, helps show the world what hacking is all about and helps feed and cultivate projects and activities going on locally and globally.... that we're not just in it for ourselves we're in it for our neighbors and our world.⁴²⁹

There is a pronounced "welcoming attitude" with makers and hackerspaces.⁴³⁰ Mitch Altman, who founded the Noisebridge hackerspace in San Francisco and was part of the group of hackers who set the hackerspace movement in motion, says, "That welcoming attitude is proving powerfully attractive to many geeks. I can go to any hacker space anywhere in the world and be welcome there".⁴³¹

Because of the mushrooming in the late 2000s of many places and sites with various names that offer the public access to tools and equipment to build things onsite, it can be quite confusing to distinguish a hackerspace from a "makerspace", a "hackspace", a "hacklab", a "fab lab", or a "techshop".⁴³² There is even an ongoing discussion as to whether it is better to append the word "hacker" or "maker" to the name of the spaces where makers hang out. Those who prefer makerspace claim that the terms "make" and "maker" are more "open and inclusive",⁴³³ whereas "hack" and "hacker" tend to be limited and

⁴²⁸ Maxigas, "Hacklabs and hackerspaces" 8.

⁴²⁹ Nick Farr, "The Rights and Obligations of Hackerspace Members"; see also Andrew Schrok, "What Keeps Hacker and Maker Spaces Going?"

⁴³⁰ Dylan Tweney, "DIY Freaks Flock to 'Hacker Spaces' Worldwide".

Dylan Tweney, "DIY Freaks Flock to 'Hacker Spaces' Worldwide".

⁴³¹ Gus Cavalcanti, "Is it a Hackerspace, Makerspace, TechShop or FabLab?"; Maxigas, "Hacklabs and hackerspaces" 1.

⁴³² Dale Dougherty, "From Hackers to Makers"; see also Artisan's Asylum, "Make a Makerspace".

⁴³³ Gus Cavalcanti, "Is it a Hackerspace, Makerspace, TechShop or FabLab?"

exclusionary.⁴³⁴ This is reminiscent of reasoning behind the shift from “free” to “open source” software where it was similarly argued that the latter term, which seemed less risky and radical, was more palatable to a broader audience. As with the debate between the labels “free” versus “open source” software, I view the debate between hackerspace and makerspace as mainly an ideological rather than a practical matter. In fact, plenty of makers refer to themselves as hackers, and they do not make any distinction between a hackerspace and a makerspace and they use the terms synonymously.⁴³⁵ There is also concern among the maker community that only those spaces that are connected to or have an agreement with the company Maker Media, which publishes MAKE magazine and organizes Maker Faire, can officially use the term makerspaces. This goes against the free and open mentality of makers.

I prefer to use the term hackerspace since it highlights the fact that these sites draw from and belong to hacker culture. While Cavalcanti prefers the term makerspaces,⁴³⁶ his description of the characteristics of hackerspaces supports my view that the term hackerspace has a closer connection to the history and culture of hacking:

In my mind, hackerspaces largely focused on repurposing hardware, working on electronic components, and programming... hackerspaces also became associated in my mind with tendencies towards collectivism, and radical democratic process as method for making decisions – an inheritance from European hackerspaces and early American hackerspaces.⁴³⁷

Whether a communal workshop occupied by makers and other hackers is officially called a makerspace, hacklab,⁴³⁸ hackerspace,⁴³⁹ or

⁴³⁴ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”.

⁴³⁵ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”; see OHM2013 (where the words hacker and maker are used together and often interchangeably).

⁴³⁶ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”.

⁴³⁷ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”.

⁴³⁸ See Maxigas, “Hacklabs and hackerspaces – tracing two genealogies” (while there are important distinctions between hackerspaces and hacklabs, I would ultimately include hacklabs under the general category of hackerspaces since they both draw from hacker culture).

⁴³⁹ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?” (in the United Kingdom, it appears that the convention is to call hackerspaces as hackerspaces).

some other name, it will be considered a hackerspace if it is grounded in, draws from or considers itself a part of hacker culture.

Distinguishing a hackerspace from a fab lab or TechShop is a simpler affair. Unlike hackerspaces which “are set up by hackers for hackers with the principal mission of supporting hacking”, the main goal of fab labs and TechShops is to “foster innovation”.⁴⁴⁰ A fab lab is short for “fabrication laboratory”⁴⁴¹ and that is part of a “global network of local labs, enabling invention by providing access to tools for digital fabrication”.⁴⁴² Neil Gerschenfeld established the first fab lab at the Center for Bits and Atoms at MIT in 2005.⁴⁴³ As conceived by Gerschenfeld, a fab lab is a place where specific tools and equipment are available for anyone to use so they can “make almost anything”.⁴⁴⁴ In contrast to hackerspaces, which are formed by a community of makers, fab labs are run by more formal organizations, but “there is no formal procedure in how to become a Fab Lab, the process is monitored by MIT, and MIT maintains a list of all Fab Labs worldwide”.⁴⁴⁵ Interestingly, fab labs share the same principles of openness and collaboration of the FOSS movement and hackerspaces; its charter “stipulates open access, establishes peer learning as a core feature and requires that designs and processes developed in fab labs must remain available for individual use”.⁴⁴⁶ Despite the organizational differences between hackerspaces and fab labs, it should be noted though that makers and other hackers also frequent fab labs and many fab labs are active in the maker scene. TechShops are commercial spaces that started in 2006. People can have access to machinist equipment and design tools such as milling machines and laser cutters by paying a

⁴⁴⁰ Maxigas, “Hacklabs and hackerspaces” 4.

⁴⁴¹ Peter Troxler, “Libraries of the Peer Production Era”.

⁴⁴² “The Fab Charter”.

⁴⁴³ Gus Cavalcanti, “Is it a Hackerspace, Makerspace, TechShop or FabLab?”; Chris Anderson, *Makers* 46.

⁴⁴⁴ Neil Gerschenfeld, “How to Make Almost Anything”; see also Chris Anderson, *Makers* 46.

⁴⁴⁵ Peter Troxler, “Libraries of the Peer Production Era”; see also Maxigas, “Hacklabs and hackerspaces” 4.

⁴⁴⁶ Peter Troxler, “Libraries of the Peer Production Era”; see also Chris Anderson, *Makers* 46.

⁴⁴⁷ Peter Troxler, “Libraries of the Peer Production Era”; see also Chris Anderson, *Makers* 46.

membership fee.⁴⁴⁷ While TechShops are open to people within a local area, they are set up and run by a for-profit company. It is important to bear in mind though that, even if hackerspaces are distinct from fab labs and TechShops, the social spheres of makers are not circumscribed exclusively to hackerspaces, and many makers and hackers do frequent other places and sites including fab labs.

2.2.6.3 MakerBot

With the increasing public attention and growing commercial interest in makers and their projects, it was inevitable that the maker movement, too, like the computer hobbyists, would have an “Apple II moment”. To the consternation of the maker community that once wholeheartedly supported it, MakerBot is aiming, in more ways than one, to be the Apple of the 3D printing revolution.⁴⁴⁸ When it was founded in 2009, the MakerBot company was an open hardware start-up that produced and sold an open source, desktop 3D printer kit.⁴⁴⁹ MakerBot had its origins in the New York hackerspace NYC Resistor: its founders Bre Pettis, Zach Smith and Adam Mayer met there, and the first prototype of the 3D printer (then called the CupCake CNC) was made in the hackerspace.⁴⁵⁰ The MakerBot 3D printer was based and built on open technologies like RepRap and Arduino.⁴⁵¹ Like the Altair, the first MakerBot 3D printer was sold as a hobbyist kit and the specifications and designs were open to anyone.⁴⁵² MakerBot was popular among makers because “[t]he machine’s modularity and its open plans make it attractive to tinkerers who are turned off by hacker-unfriendly ‘black box’ technologies”.⁴⁵³ Because the MakerBot

⁴⁴⁸ Rob Giseburt, “MakerBot’s Mixed Messages About Open Source, Their Future”; Chris Anderson, “The New MakerBot Replicator Might Just Change Your World”; Chris Anderson, *Makers* 20.

⁴⁴⁹ Ken Denmead, “MakerBot Origins”.

⁴⁵⁰ Ken Denmead, “MakerBot Origins”; Walter, “The Makerbot/Thingiverse move to the Dark Side”; Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”.

⁴⁵¹ Ken Denmead, “MakerBot Origins”; Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”; Chris Anderson, *Makers* 107.

⁴⁵² Ken Denmead, “MakerBot Origins”.

⁴⁵³ Ken Denmead, “MakerBot Origins”.

hardware was open, “[a]s owners of previous batches build and use their machines, they make suggestions and improvements to the design of the machine. These improvements are implemented in future batches, and made available to current users as an upgrade”.⁴⁵⁴ Aside from hardware, the software and community surrounding MakerBot embraced free sharing and collaboration.⁴⁵⁵ The MakerBot community used free software and open standards such as Skeinforge, ReplicatorG, Art of Illusion, and Blender (the latter two are 3D design and modeling programs).⁴⁵⁶ The Thingiverse website, which Pettis started in 2008, helped community members communicate, share and collaborate online.⁴⁵⁷ Like FOSS developers, users on the Thingiverse website could share their 3D designs and other source files, have other users modify and improve the files, and make everything available to the public.⁴⁵⁸

The creators and founders of MakerBot were stalwarts in the maker community and championed openness.⁴⁵⁹ Pettis was part of the group that jumpstarted the hackerspace movement in the United States,⁴⁶⁰ and Zach Smith was a founding member of RepRap and designed its motherboard.⁴⁶¹ The MakerBot company and its eponymous 3D printer were the darlings and poster children of the maker movement because, like Linux, they were concrete proof that a company could openly share and make public all of its technical know-how and innovations and produce a great product at a reasonable price, while still being a viable business.⁴⁶² MakerBot was at the forefront of democratizing 3D printing.⁴⁶³ True to the hacker spirit, Pettis once

⁴⁵⁴ Ken Denmead, “MakerBot Origins”; see also Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”.

⁴⁵⁵ Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”.

⁴⁵⁶ Ken Denmead, “MakerBot Origins”.

⁴⁵⁷ Ken Denmead, “MakerBot Origins”.

⁴⁵⁸ Ken Denmead, “MakerBot Origins”; Chris Anderson, *Makers* 72-74.

⁴⁵⁹ Bre Pettis, “Open Source Ethics and Dead End Derivatives”.

⁴⁶⁰ Dylan Tweney, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide”.

⁴⁶¹ Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”; Ken Denmead, “MakerBot Origins”; Hackerspaces - The Beginning 99.

⁴⁶² See Ashlee Vance, “Bre Pettis: 3D Printing’s First Celebrity”; Ken Denmead, “MakerBot Origins”; Phillip Torrone, “Life, \$10M in Funding, and Beyond”; Chris Anderson, *Makers* 108.

⁴⁶³ Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”.

empathically stated:

At MakerBot, we take open source seriously. It's a way of life for us. We share our design files when we release a project because we know that it's important for our users to know that a MakerBot is not a black box. With MakerBot, you get not only the machine that makes things for you, but you also get an education into how the machine works and you can truly own it and have access to all the designs that went into it! When people take designs that are open and they close them, they are creating a dead end where people will not be able to understand their machine and they will not be able to develop on them.⁴⁶⁴

It thus came as a great surprise to the maker community when MakerBot did not release as open source the hardware designs and software code of its “Replicator 2” desktop 3D printer in 2012.⁴⁶⁵ MakerBot's reversal of its community outlook and commercial and legal strategy (including how it protected, licensed and exploited its intellectual property and technical know-how) seriously affected the maker community, and it caused a great degree of divisiveness, outrage, heated debate and soul searching among makers.⁴⁶⁶ Co-founder Zach Smith, who was at the time no longer part of the MakerBot company, severely criticized MakerBot's closure and called it “the ultimate betrayal”.⁴⁶⁷ Community members felt that MakerBot had “lost touch with the way that open source is supposed to work, and the core principles that the company was built upon”.⁴⁶⁸ As with the PC, business reasons and commercial interests were behind MakerBot's shift from free and open to proprietary and closed.⁴⁶⁹ MakerBot had received

⁴⁶⁴ Bre Pettis, “Open Source Ethics and Dead End Derivatives”; see also Phillip Torrone, “Life, \$10M in Funding, and Beyond”.

⁴⁶⁵ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”; Bre Pettis, “Let's try that again”; Walter, “The Makerbot/Thingiverse move to the Dark Side”.

⁴⁶⁶ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”; Josef Prusa, “Occupy Thingiverse Test cube”, Thingiverse; Bre Pettis, “Fixing Misinformation with Information”; Bre Pettis, “Let's try that again”; Walter, “The Makerbot/Thingiverse move to the Dark Side”; Bre Pettis, “Thingiverse updates Terms of Use and License options”; Richard McCarthy, “Our Lawyer Explains the Thingiverse Terms of Service”; John Baichtal, “Brazilian 3D Printer Company Weighs in on the Makerbot controversy”; Tigoe, “In defense of open source innovation and polite disagreement”.

⁴⁶⁷ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their

⁴⁶⁸ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”; see also Walter, “The Makerbot/Thingiverse move to the Dark Side”.

⁴⁶⁹ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”; Bre Pettis, “Fixing Misinformation with Information”; Bre Pettis, “Let's try that again”; Rob Giseburt, “Is One of Our Open Source Heroes Going Closed Source?”.

⁴⁷⁰ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”; Bre Pettis, “Let's try that again”; Walter, “The Makerbot/Thingiverse move to the Dark Side”; Phillip Torrone, “Life, \$10M in Funding, and Beyond”; Chris Anderson, Makers 95.

US\$10 million in outside venture capital funding,⁴⁷⁰ and the Replicator 2 was the company's serious attempt to market a consumer-friendly 3D printer for the mass market with no assembly required (as the Apple II was for PCs).⁴⁷¹

Rather than sharing everything and being completely open, MakerBot would only “share as much as possible” and be “as open as possible and still have a business at the end of the day”.⁴⁷² As a result of the changed outlook, MakerBot would “not share the way the physical machine is designed or our GUI” as it had done with the previous generations of the 3D printer.⁴⁷³ Echoing Steve Jobs's defense of the merits of Apple's centrally controlled and curated model to developing technologies (versus the open yet chaotic approach of rivals),⁴⁷⁴ Pettis states, “We've transitioned to a company that makes a tool, the MakerBot Replicator 2, that has set a new standard in desktop 3D printing because it just works.... It's a paradox because all this makes the hardware less hacker friendly, but more user friendly”.⁴⁷⁵ Exposed to the pressures of business and the demands of making profits, openness was no longer seen by MakerBot as a clear advantage but rather a weakness.⁴⁷⁶ Pettis says, “I don't plan on letting the vulnerabilities of being open hardware destroy what we've created”.⁴⁷⁷ Reminiscent of Bill Gates's letter to computer hobbyists, Pettis wrote in a blog post, “If this is how the community treats a company that has shared a lot, it will be harder for other businesses and projects to choose open source as a way of sharing their work”.⁴⁷⁸ Many makers felt betrayed when MakerBot turned its back on open source and the maker community.⁴⁷⁹ As Giseburt explains, “Makers don't like black-box trinkets. They

⁴⁷¹ Bre Pettis, “Fixing Misinformation with Information”; Bre Pettis, “Let's try that again”.

⁴⁷² Bre Pettis, “Fixing Misinformation with Information”; see also Walter, “The Makerbot/Thingiverse move to the Dark Side”.

⁴⁷³ Bre Pettis, “Let's try that again”; see also “GUT”, Computer Desktop Encyclopedia (GUI is short for “Graphical User Interface” and is “the common method of interacting with a computer that allows any graphics image to be displayed on screen”).

⁴⁷⁴ Tim Wu, “Does a Company Like Apple Need a Genius Like Steve Jobs”.

⁴⁷⁵ Bre Pettis, “Let's try that again” (emphasis added).

⁴⁷⁶ Bre Pettis, “Fixing Misinformation with Information”.

⁴⁷⁷ Bre Pettis, “Fixing Misinformation with Information”.

⁴⁷⁸ Bre Pettis, “Let's try that again”.

⁴⁷⁹ Rob Giseburt, “MakerBot's Mixed Messages About Open Source, Their Future”.

want something that, if they want to open it up and learn how it works, they can. They can also... scratch their own itch and solve whatever problem they are having, furthering the technology for the entire community".⁴⁸⁰ Financially speaking, like Apple, MakerBot's decision to become less open and more commercial appears to have paid off. In 2013, Stratasys, a major industrial 3D printer manufacturer, acquired MakerBot for US\$403 million.⁴⁸¹

Despite the controversies and debates surrounding MakerBot's closure and the impact of military funding of hackerspaces in the United States,⁴⁸² makers continue to build and work hard to ensure that the community and their projects remain free and open to all. Thanks in large part to the success and experience of hackers with the FOSS movement, the current situation is much better when compared to the state of computing and hacking in the early 1980s. Unlike the MIT hackers and computer hobbyists, makers today have a wide range of open technologies, platforms and standards that are available and accessible to them such as RepRap, Arduino and Linux. There are also many thriving technology companies like Adafruit, SparkFun, GitHub and Ubuntu that choose to open everything or "open source (almost) everything".⁴⁸³ So even if companies like MakerBot decide to make their succeeding products and services proprietary and closed, it will not affect the many makers who prefer to work with and build on truly open projects. Further, since a number of these maker projects are released under copyleft licenses like the GPL, the freedom and openness of the underlying technologies are protected and guaranteed by the one-two punch of legal rules and social norms.⁴⁸⁴

⁴⁸⁰ Rob Giseburt, "Is One of Our Open Source Heroes Going Closed Source?"

⁴⁸¹ Stratasys, "Stratasys to Acquire MakerBot, Merging Two Global 3D Printing Industry Leaders"; D.C. Denison, "Reactions to the MakerBot-Stratasys Deal".

⁴⁸² Mitch Altman, "Hacking at the Crossroad: US Military Funding of Hackerspaces" (which is eerily similar to the US government's funding of the early MIT computer hackers).

⁴⁸³ Tom Preston-Werner, "Open Source (Almost) Everything"; see also Peter Troxler, "Libraries of the Peer Production Era"; see also Chris Anderson, *Makers* 19 and 107.

⁴⁸⁴ See Phillip Torrone, "The (Unspoken) Rules of Open Source Hardware"; Bre Pettis, "Open Source Ethics and Dead End Derivatives".

2.3 Makers and hacktivists in context

Viewed from the panorama of hacker history and culture, it is easier to understand the relative position and orientation of makers and hacktivists in relation to the various hacker types and periods. Hacker culture and the different types of hackers clearly have a strong influence and impact on both makers and hacktivists. Like the other hacker types, makers and hacktivists are extremely passionate about technology, desire to gain expertise and mastery over it, and wish to use technology in new, innovate and unexpected ways. There is also a decidedly rebellious and non-conformist streak that runs through all types of hackers. Makers in particular continue the hacker tradition and practice of creatively using technology. But unlike the early computer scientists and programmers, makers are not only interested in hacking computer hardware, software and systems but all forms of technology. Nothing is off limits to hacking, not even biology or their own bodies.⁴⁸⁵ With computer hobbyists, makers share the same curiosity and enthusiasm to learn more about, create and develop technologies like 3D printers. They do so not just for their own satisfaction but in order to benefit other makers and the public. Makers hope to ignite their own version of the PC revolution but this time with 3D printers and other digital manufacturing tools. Like the computer hobbyists, makers see the importance of meeting in person, sharing and working with others on their projects. But makers have gone beyond the casual club meetings of computer hobbyists and they have set up their own hackerspaces where they can hang out and hack with others. As with the computer hobbyists, they also greatly value free and open access to and use of information and technologies. Carrying on the praxis and goals of FOSS developers, makers similarly seek to keep their technologies and projects free for others to use and re-use by

⁴⁸⁵ See Sara Tocchetti, "DIYbiologists as 'makers' of personal biologics"; Denisa Kera, "Hackerspaces and DIYbio in Asia".

releasing them under FOSS licenses. Of course, as with the early computer scientists and computer hobbyists, they too face conflicts and tensions within their community when some of their members seek to assert and enforce intellectual property rights exclusively for personal profit or commercial gain.

Hactivists, on the other hand, also possess the same anti-establishment attitude and countercultural goals of early computer scientists and computer hobbyists. But they do not consider technology to be an end in itself but as a powerful means for socio-political ends. Hactivists have an affinity with underground hackers who similarly used information systems to build their communities and also to cause disruption and change in the wider world. In the same way that BBSes were at the center of the activities and interactions of underground hackers, hactivists primarily use the internet for coordinating and carrying out their campaigns. But while underground hackers sometimes carried out acts of rebellion for its own sake or against what they perceived to be faceless authorities or monolithic bureaucracies, hactivists undertake acts of hacktivism for more pressing or serious causes such as supporting oppressed groups or campaigning for human rights. While all hackers types are community oriented and possess some degree of social awareness, hactivists are the most politicized and socially active among them. Because hactivists push the boundaries the most in order to produce socio-political change, they are more likely to run afoul of the law and be the subject of legal prosecution than other hackers. While they also enjoy messing around with technology, hactivists always have larger goals in mind and they seek to combine the technical and social domains with virtual and physical action. Hactivists also believe in the ideals of FOSS developers and the technologies and systems they use are almost exclusively open source.

The preceding narrative about different hacker types and pe-

riods is not only valuable in how it properly situates makers and hacktivists within hacker culture, but it also reveals the recurring and dialectical conflicts that concern hacking. Aside from the perennial conflict between free and open versus proprietary and closed, another discernable tension is the contrasting policies that the law and public authorities take in relation to hacking: proscribing and prosecuting hacking activities as opposed to tolerating and encouraging them (restrict versus support). A further issue area is the distinct attitudes and responses that hackers have to law and public authorities – i.e., whether hackers choose to conform to the existing legal order or to avoid or creatively subvert it as FOSS developers have done (conformity versus non-conformity). With regard to their social orientation and involvement, there is a clear divergence between hackers who wish to remain isolated within and solely focused on their internal domains, and those who are socially and outwardly oriented and desire to engage with and change the wider world (individual autonomy versus community and social responsibility). Together with the breaking and making dynamic that pervades hacker culture, these themes continually arise throughout hacker history and so too with makers and hacktivists. The above conflicts come into sharper focus when viewed from the perspective of hacker norms and values, which are the subject of the next chapter.

CHAPTER THREE

Hacker norms and values

This chapter examines the social norms and values of makers and hacktivists. The study of norms and values is crucial for comprehending who makers and hacktivists are and why they respond to law and public authorities in the way they do. As explained below, hacker norms and values help explain the reasons and motivations for their behaviors and actions. Furthermore, their norms and values are embodied and enacted in their technologies and activities. The norms and values that are described in this chapter were observed and collected through interviews with members of the hacker community, participant observation at hackerspaces and hacker events, and content analysis of manifestos written by and about hackers. The process of determining and understanding their norms and values is additionally useful because it produces a more intimate, grounded and empathetic view of makers and hacktivists.

3.1 The why of hacking

Makers and hacktivists share numerous similarities with other types of hackers who make up hacker culture. Of the manifold elements and dimensions of hacker culture, norms and values are extremely relevant and crucial in determining how and why makers and hacktivists interact with technology laws. In justifying the importance of social norms to law, Etzioni states, “the study of social norms is of considerable importance for the full study of law” since “social norms affect behavior in general and the law specifically”.¹ Posner is similarly

¹Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 160 and 162.

unequivocal: “A full understanding of law requires consideration of norms”.² Examining their norms and values can help elucidate hackers’ actions, beliefs and attitudes, especially in relation to technology law and policy.³ While Chapter 2 delved into what hackers did, where they hacked, and how the law and authorities viewed and responded to them, this chapter seeks to explain the why of hacking by examining makers’ and hacktivists’ norms and values.

3.2 Conceptual elaborations

Norms and values are complex and contested concepts, and precise definitions of these terms are much debated within and across scholarly disciplines.⁴ It is not the aim of this book to resolve these intractable theoretical and definitional discussions.⁵ While norms and values can be defined and explained in various ways,⁶ as explained in the succeeding sections, I adopt a sociology-based conceptualization of these two core concepts because the main focus of the research is the social behaviors and beliefs of hacker groups and communities.⁷

3.2.1 NORMS

A social norm (or norm for short) has been defined as “a statement made by a number of members of a group, not necessarily by all of them, that the members ought to behave in a certain way in certain circumstances”.⁸ It is also described as “a belief shared to some extent by members of a social unit as to what conduct ought to be in partic-

² Richard Posner, “Social Norms and the Law: An Economic Approach” 365.

³ Jack Gibbs, Norms, Deviance, and Social Control 2 and 16.

⁴ Jack Gibbs, Norms, Deviance, and Social Control 9 and 19; Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 394; Michael Hechter and Karl-Dieter Opp “Social Norms” xiii, 396 and 402; Richard McAdams and Eric Rasmusen, “Norms and the Law” 1576.

⁵ Jack Gibbs, Norms, Deviance, and Social Control x and 9; James Spates, “The Sociology of Values” 35-36; Michael Hechter, “Should Values Be Written Out of the Social Scientist’s Lexicon” 217-219.

⁶ Jack Gibbs, “Norms: The Problem of Definition and Classification” 587.

⁷ See Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 158; Richard McAdams and Eric Rasmusen, “Norms and the Law” 1576.

⁸ Jack Gibbs, Norms, Deviance, and Social Control 8; see K.D. Opp “Norms” 10714.

ular situations or circumstances”.⁹ Norms are considered “generally accepted, sanctioned prescriptions for, or prohibitions against, others’ behavior..., i.e. what others ought to do... or else”.¹⁰ According to Gibbs, a social norm on the whole “involves: (1) a collective evaluation of behavior in terms of what it ought to be; (2) a collective expectation as to what behavior will be; and/or (3) particular reactions to behavior, including attempts to apply sanctions or otherwise induce a particular kind of conduct”.¹¹ Dohrenwend defines a social norm as:

a rule which, over a period of time, proves binding on the overt behavior of each individual in an aggregate of two or more individuals. It is marked by the following characteristics: (1) Being a rule, it has content known to at least one member of the social aggregate. (2) Being a binding rule, it regulates the behavior of any given individual in the social aggregate by virtue of (a) his [or her] having internalized the rule; (b) external sanctions in support of the rule applied to him [or her] by one or more other individuals in the social aggregate; (c) external sanctions in support of the rule applied to him [or her] by an authority outside the social aggregate; or any combination of these circumstances.¹²

I am inclined to use Dohrenwend’s definition as it is more detailed and complete compared to other definitions.¹³ Further, it underscores the key attributes of a social norm: it takes the form of a rule; possesses an element of regularity; is considered binding or carries a sense of oughtness; is based on shared expectations and evaluations; influences behavior; has internal and external dimensions; and involves sanctions or inducements of some kind.¹⁴ It bears stressing that in this book the term norm is used as shorthand for social norms and these terms have

⁹ Jack Gibbs, *Norms, Deviance, and Social Control* 7.

¹⁰ Richard Morris, “A Typology of Norms” 610.

¹¹ Jack Gibbs, “Norms: The Problem of Definition and Classification” 589 and 594; see Jack Gibbs, *Norms, Deviance, and Social Control* 18.

¹² Bruce Dohrenwend, “A Conceptual Analysis of Durkheim’s Types” 470.

¹³ Jack Gibbs, “Norms: The Problem of Definition and Classification” 587-588.

¹⁴ Bruce Dohrenwend, “A Conceptual Analysis of Durkheim’s Types” 470 and 472; K.D. Opp “Norms” 10714; Jack Gibbs, *Norms, Deviance, and Social Control* 3; Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 167; Michael Hechter and Karl-Dieter Opp, *Social Norms* xi, 403 and 404; Christine Horne, “Sociological Perspectives on the Emergence of Social Norms” 5; Michael Baumann and others, *Norms and Values* 9.

the same meaning and are used interchangeably.

In terms of classification, there are three main types of social norms: “mores, customs and laws”.¹⁵ Mores are “collective beliefs as to how persons ought to behave ... they relate to certain kinds of conduct which are deemed so important to social welfare that they are defended overtly”,¹⁶ while customs are “collective expectations as to what persons actually do and not beliefs as to what they should do”.¹⁷ It is important to bear in mind that from the viewpoint of the social sciences, law is held to be “a type of norm” and a subset within the broad category of social norms.¹⁸ While law resists a precise and untested definition even in the field of jurisprudence and legal science, law is generally understood in sociology in this way: “An order will be called law if it is externally guaranteed by the probability that coercion (physical or psychological), to bring about conformity or avenge violation, will be applied by a staff of people holding themselves specifically ready for that purpose”.¹⁹ As Gibbs further explains, “A law is enforced by persons in special statuses through means that may include the use of force with a low probability of retaliation, a condition that does not characterize customs, mores”.²⁰ The relation between social norms and law can be described in terms of their varying degrees of formality, importance, certainty and generality.²¹ As social norms, laws would be those that are more formal, serious, coercive, forcefully applied, and comprehensive in their application.

While it may be said that laws are simply more formal social norms that are promulgated and enforced in a special manner, it is

¹⁵ Jack Gibbs, *Norms, Deviance, and Social Control* 17; but see Jack Gibbs, “Norms: The Problem of Definition and Classification” 587-588 and 591-592; and Richard Morris, “A Typology of Norms” 610-612 (who provides a more extensive list that include “folkways, mores, customary law, enacted law, custom” as part of the overall typology of norms).

¹⁶ Jack Gibbs, “Norms: The Problem of Definition and Classification” 592-593; see also Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 388.

¹⁷ Jack Gibbs, “Norms: The Problem of Definition and Classification” 592-593.

¹⁸ Jack Gibbs, “The Sociology of Law and Normative Phenomena” 315; K.D. Opp “Norms” 10715; Richard Posner, “Social Norms and the Law” 365.

¹⁹ Jack Gibbs, “Norms: The Problem of Definition and Classification” 590 (citing Max Weber); see also K.D. Opp “Norms” 10715.

²⁰ Jack Gibbs, “The Sociology of Law and Normative Phenomena” 316.

²¹ Michael Dizon, “Rules of a networked society” 87.

still necessary to treat law as discrete from social norms.²² According to Hechter and Opp, laws and social norms can be distinguished in the following manner:

Although the law, too, relies on norms, [laws] are different from social norms. [Laws] are created by design – usually through some kind of deliberative process, precisely specified in written texts, linked to particular sanctions, and enforced by a specialized bureaucracy. Social norms, by contrast, often are spontaneous rather than deliberately planned (hence, of uncertain origin), unwritten (hence, their content and rules for application are often imprecise), and enforced informally (although the resulting sanctions can sometimes be a matter of life and death).²³

Lessig's much cited and applied model of the four modalities of regulation similarly treats law and social norms as interconnected yet separate concepts.²⁴ Keeping law as a distinct concept is important since, even in a globalizing and increasingly networked world, law remains a powerful and vital source and resource of rules, sanctions and inducements that impact and shape human action and social behavior.²⁵ As such, rather than conflating law and social norms, being cognizant of their similarities, differences and interactions can help provide “conceptual clarity” as well as produce practical results for both legal and social research.²⁶ Scholars on both sides agree that the relationship and interactions between social norms and laws are “complexly intertwined”.²⁷ Etzioni explains one such relation between laws and social norms that may have a valuable import for public authorities attempting to maintain social order or influence social behavior:

²² D.J. Galligan, *Law in Modern Society* 188; Jane Ruby, “The Origin of Scientific Laws” 591; see Michael Dizon, “Rules of a networked society” 84-87 (for a more detailed explanation of the relationship between law and norms).

²³ Michael Hechter and Karl-Dieter Opp “Social Norms” xi.

²⁴ Lawrence Lessig, *Code* 123.

²⁵ Sally Falk Moore, “Law and Social Change” 745; see Anne Griffith, “Legal Pluralism” 301-302; see Richard McAdams and Eric Rasmusen, “Norms and the Law” 1589, 1593, 1596 and 1609 (on the law’s ability to change, improve or work better than norms in certain cases); see Robert Cooter, “Normative Failure Theory of Law” 948, 949 and 979; see F.A. Hayek, *Law, Legislation and Liberty: Volume I Rules and Order* 88.

²⁶ Jack Gibbs, “The Sociology of Law and Normative Phenomena” 316.

²⁷ Robert Ellickson, “The Evolution of Social Norms” 62; see also Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 159; see also Jack Gibbs, “The Sociology of Law and Normative Phenomena” 322; see also Richard Posner, “Social Norms and the Law” 365.

it is widely held that strong social norms reduce the burden of law enforcement; that laws supported by social norms are likely to be significantly more enforceable; and that laws that are formulated in ways that are congruent with social norms are much more likely to be enacted than laws that offend such norms.²⁸

3.2.2 VALUES

Values are closely connected to norms but remain a discrete concept. According to Kluckhohn's widely cited and influential definition, "A value is a conception, explicit or implicit, distinctive of an individual or characteristic of a group, of the desirable which influences the selection from available modes, means, and ends of action".²⁹ Rokeach similarly defines a value as "an enduring prescriptive or proscriptive belief that a specific mode of behavior or end-state of existence is preferred to an opposite or converse mode of behavior or end-state".³⁰ The "desirable" as opposed to "the desired" is a key notion in the concept of values since "[t]he desirable is what it is felt or thought proper to want. It is what an actor or group of actors desire – and believe they 'ought' or 'should' desire – for the individual or a plurality of individuals".³¹ With regard to its characteristics, a value: is a "prescriptive or proscriptive belief"; is enduring yet subject to change; competes with other values (and is thus naturally subject to negotiation, balancing and prioritization); has "cognitive, affective and behavioral components"; and has conflict-resolution, decision-making and expressive functions.³² According to Rokeach, there are two kinds of values: instrumental values, which pertain to modes of conduct; and

²⁸ Amitai Etzioni, "Social norms: Internalization, Persuasion, and History" 159.

²⁹ Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 395; see also Milton Rokeach, *The Nature of Human Values* 9; see also Richard Morris, "A Typology of Norms" 610; see also Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 362; see also James Spates, "The Sociology of Values" 30.

³⁰ Milton Rokeach, *The Nature of Human Values* 5 and 25; see also Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 362; but see Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 403 (who states that "the distinction between ends and means is somewhat transitory, depending upon time perspective"); see also Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 366.

³¹ Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 396.

³² Milton Rokeach, *The Nature of Human Values* 6, 7, 12, 20 and 25; see also Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 395-396.

terminal values, which refer to end-states of existence.³³ Examples of instrumental values in Rokeach's study of American values include honesty, independence, and ambition, whereas equality, freedom and security are terminal values.³⁴ With regard to their operation, instrumental and terminal values "represent two separate yet functionally interconnected systems, wherein all the values concerning modes of behavior are instrumental to the attainment of all the values concerning end-states".³⁵ It should be noted that other scholars are of the view that there should be no distinction between instrumental and terminal values since "the same values can express motivations for both means and ends".³⁶ As a standard of action, evaluation, and rationalization, a value guides conduct and determines an individual's or group's action.³⁷ Based on existing literature, the five common features of values are "(a) concepts or beliefs, (b) about desirable end states or behaviors, (c) that transcend specific situations, (d) guide selection or evaluation of behavior and events, and (e) are ordered by relative importance".³⁸

Values are distinguishable from norms since "ideas of what is desirable [are] distinct from shared ideas of what others ought to do, with sanctions attached".³⁹ While values can be "personal and internal", norms are consensual and interpersonal.⁴⁰ As such, "[v]alues can be held by a single individual; norms cannot. Norms must be shared prescriptions and apply to others, by definition".⁴¹ Furthermore, "[v]alues have only a subject – the believer – while norms have both subject and objects – those who set the prescription, and those to whom it applies".⁴² Importantly, norms involve sanctions and incentives but values per se do not have to.⁴³

³³ Milton Rokeach, *The Nature of Human Values* 7-8; Michael Hechter, "Should Values Be Written Out of the Social Scientist's Lexicon" 216.

³⁴ Milton Rokeach, *The Nature of Human Values* 28.

³⁵ Milton Rokeach, *The Nature of Human Values* 12.

³⁶ Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept".

³⁷ Milton Rokeach, *The Nature of Human Values* 13-14; Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 379.

³⁸ Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 362.

³⁹ Richard Morris, "A Typology of Norms" 611.

⁴⁰ Milton Rokeach, *The Nature of Human Values* 19.

⁴¹ Richard Morris, "A Typology of Norms" 610.

Despite their conceptual distinctions, norms and values are intimately interconnected to each other. Norms are frequently linked to and defined in relation to values.⁴⁴ For Giddens, norms are “[r]ules of behaviour that reflect or embody a culture’s values, either prescribing a given type of behaviour, or forbidding it”.⁴⁵ Gibbs likewise asserts that “[n]orms are based on cultural values”.⁴⁶ The very notion of collective evaluations and expectations “implies the existence of shared values”;⁴⁷ and values likewise concern normative propositions.⁴⁸ It is often the case that “[v]alue statements are... normative statements” as well.⁴⁹ The relationship between norms and values can thus be best described as symbiotic since “most norms are based upon established values” and “commonly held values often result in the formation of norms that insure the maintenance of [those] values”.⁵⁰ Their inherent conceptual and empirical closeness may explain why they are commonly spoken of or analyzed together as simply “norms and values”.⁵¹

3.3 Manifestations of norms and values

3.3.1 MANIFESTOS

Hacker norms and values can be discerned from their written statements and other writings about their culture. One benefit of studying hackers is that, regardless of their type, they seemingly have no reservations or inhibitions about putting down in writing and making public their beliefs, experiences and views about techno-social

⁴² Richard Morris, “A Typology of Norms” 610.

⁴³ Richard Morris, “A Typology of Norms” 610; Michael Hechter, “Should Values Be Written Out of the Social Scientist’s Lexicon” 215.

⁴⁴ Gary Fine, “Enacting Norms” 161; Christine Horne, “Sociological Perspectives on the Emergence of Social Norms” 4; Michael Baumann and others, Norms and Values 7 and 10.

⁴⁵ Anthony Giddens, *Sociology* 1127 (emphasis added).

⁴⁶ Jack Gibbs, “Norms: The Problem of Definition and Classification” 586.

⁴⁷ Jack Gibbs, “Norms: The Problem of Definition and Classification” 589.

⁴⁸ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 390.

⁴⁹ Clyde Kluckhohn and others, “Values and Value-Orientations in the Theory of Action” 398; see also Steven Hitlin and Jane Piliavin, “Values: Reviving a Dormant Concept” 379.

⁵⁰ Richard Morris, “A Typology of Norms” 610; Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 174.

⁵¹ Steven Hitlin and Jane Piliavin, “Values: Reviving a Dormant Concept” 359.

issues, including statements about the normative and the desirable. In fact, given the profusion of emphatic writings by hackers about their culture, it may even be said that they revel in expressing themselves through writing almost as much as they do developing code and technical innovations. Of the many texts and documents that have been written by or on behalf of hackers, the manifesto has proven to be a popular genre to express and enact their norms and values. Hacker manifestos can therefore serve as valuable sources and materials for examining and understanding hackers' conceptions and evaluations of and responses to what they consider acceptable conduct and desirable goals.

Manifestos are particularly suited for examining and confirming hacker norms and values since these manifestary texts are indisputably normative and aspirational.⁵² While manifestos articulate and affirm certain norms and values,⁵³ they similarly transgress and transform other rules and standards of the acceptable and desirable both within and outside the manifesto writer's social world.⁵⁴ According to Yanoshevsky, "The term manifesto, strictly speaking, applies to (often short) texts published in a brochure, in a journal or a review, in the name of a political, philosophical, literary or artistic movement".⁵⁵ The manifesto can take on "different shapes and forms"⁵⁶ such as decrees, declarations, proclamations, petitions, pamphlets, flyers, open letters and appeals to action.⁵⁷ A text can be a manifesto even if it is not labeled as such, and the determining factor is whether the text possesses "manifestary" elements and characteristics.⁵⁸

⁵² Teresa Ebert, "Manifesto as Theory" 556; Martin Puchner, "Manifesto = Theatre" 452.

⁵³ Galia Yanoshevsky, "The Decades of Writing on Manifesto" 268.

⁵⁴ Teresa Ebert, "Manifesto as Theory" 556.

⁵⁵ Galia Yanoshevsky, "Three Decades of Writing on Manifesto" 261 (citing Abastado); Brian Fauteux, "Manifestos and The Shape of Punk to Come" 466.

⁵⁶ Galia Yanoshevsky, "The Decades of Writing on Manifesto" 260.

⁵⁷ Galia Yanoshevsky, "Three Decades of Writing on Manifesto" 262-263.

A manifesto is traditionally “written collaboratively by a [fringe or marginalized] group and always on behalf of [that] group” who speaks of “We” versus “They”.⁵⁹ It is generally written in short, urgent prose while preserving a certain literary and poetic style.⁶⁰ A manifesto often contains numbered theses or bulleted lists of the movement’s key principles, statements and ideals.⁶¹ It has a hortatory and rhetorical style that is coupled with a combative or oppositional tone.⁶² Whether through the use of texts, graphics or language, its form is striking, exaggerated or aggressive,⁶³ and it is meant for broad and mass distribution.⁶⁴

With respect to function and substance, manifestos are considered a species of polemical and critical discourse.⁶⁵ Their aims are transgressive and transformative,⁶⁶ they are normally written during times of social crises and upheaval,⁶⁷ and they carry out this struggle through programs or instructions for radical change.⁶⁸ As Puchner states, “The manifesto has been geared toward a revolution, a cut in the historical process, an act that attempts to change suddenly the course of history”.⁶⁹ A manifesto has a unique quality in that it brings about what is called the “manifesto moment” or “moment of action”, which “positions itself between what has been done and what will be done, between the accomplished and the potential, in a radical and energizing division”.⁷⁰ At this moment of action, the manifesto fuses

⁵⁸ Galia Yanoshevsky, “The Decades of Writing on Manifesto” 261, 262 and 265.

⁵⁹ Martin Puchner, “Manifesto = Theatre” 455; see also Mary Ann Caws, Manifesto xx and xxiii; see also Galia Yanoshevsky, “The Decades of Writing on Manifesto” 279 and 282.

⁶⁰ Mary Ann Caws, Manifesto xxi, xxiii and xxvii; Martin Puchner, “Manifesto = Theatre” 451 and 464; Galia Yanoshevsky, “The Decades of Writing on Manifesto” 264.

⁶¹ Mary Ann Caws, Manifesto xxvi; Martin Puchner, “Manifesto = Theatre” 451; Natalie Alvarez and Jenn Stephenson, “A Manifesto for Manifestos” 4.

⁶² Galia Yanoshevsky, “The Decades of Writing on Manifesto” 266; Mary Ann Caws, Manifesto xxi, xxiii and xxvii.

⁶³ Mary Ann Caws, Manifesto xix and xx; Martin Puchner, “Manifesto = Theatre” 451 and 455; Galia Yanoshevsky, “The Decades of Writing on Manifesto” 260 and 276.

⁶⁴ Martin Puchner, “Manifesto = Theatre” 451.; Mary Ann Caws, Manifesto xix.

⁶⁵ Galia Yanoshevsky, “The Decades of Writing on Manifesto” 261-263; Teresa Ebert, “Manifesto as Theory” 554.

⁶⁶ Nanna Bisberg, “The Manifesto. Negotiating Reality” 1; Teresa Ebert, “Manifesto as Theory” 554 and 556.

⁶⁷ Galia Yanoshevsky, “The Decades of Writing on Manifesto” 263; Mary Ann Caws, Manifesto xxiii (who says that manifestos can also define a moment of crisis).

⁶⁸ Brian Fauteux, “Manifestos and The Shape of Punk to Come” 467; Galia Yanoshevsky, “The Decades of Writing on Manifesto” 268; Teresa Ebert, “Manifesto as Theory” 553.

⁶⁹ Martin Puchner, “Manifesto = Theatre” 451.

the past, present and future, and it imagines and strives to actualize the future now.⁷¹ Manifestos therefore embody and enact existing and/or aspired for norms and values. It is no wonder then that manifestos are written in both present and future tenses.⁷² As a result of this time bending and compressing property of manifestos, “All previous history becomes a preparation for this point zero, which itself is pregnant with futurity; the present act of revolt is the beginning of a new future”.⁷³

The nature and characteristics of manifestos help explain why there has been a long tradition of manifesto making among hackers. For individuals and groups who are used to harnessing technical codes and instructions to transform their environment, the idea of “chang[ing] reality with words” is both logical and appealing.⁷⁴ Hackers have always been viewed by mainstream society as subcultures or fringe groups. And, as seen in Chapter 2, all the different hackers types experienced periods of crisis and change where it was critical for them to affirm to themselves or assert to others their group identity and culture.⁷⁵ Table 3 contains an extensive although non-exhaustive list of hacker manifestos, which are organized chronologically and according to the pertinent hacker type. Even from the titles alone, the revolutionary and creative-disruptive aims and ways of hackers are readily apparent.

Due to the great number and variety of hacker manifestos, it would require a separate book to discuss the relationship between hacker culture and manifestos in complete detail. However, the normative and aspirational dimensions of manifestos for makers

⁷⁰ Mary Ann Caws, *Manifesto* xxi; Nanna Bisberg, “The Manifesto. Negotiating Reality” 34.

⁷¹ Brian Fauteux, “Manifestos and The Shape of Punk to Come” 468; Nanna Bisberg, “The Manifesto. Negotiating Reality” 2-3.

⁷² Nanna Bisberg, “The Manifesto. Negotiating Reality” 3; Mary Ann Caws, *Manifesto* xxvi.

⁷³ Martin Puchner, “Manifesto = Theatre” 452; see also Brian Fauteux, “Manifestos and The Shape of Punk to Come” 468 and 473.

⁷⁴ Galia Yanoshevsky, “The Decades of Writing on Manifesto” 264.

⁷⁵ See Goran Therborn, “Back to Norms!” 869.

and hacktivists can be sufficiently examined through a qualitative content analysis of certain representative documents. Resort to qualitative content analysis is appropriate given that its primary goals are to contextualize and to explicate the meanings and interpretations of the individuals and groups that produced particular documents.⁷⁶ This research method examines both the text and the context of a document,⁷⁷ and is thus a useful tool for discerning the norms and values of makers and hacktivists.

⁷⁶ Alan Bryman, *Social Research Methods* 418; John Scott, *A Matter of Record* 30-31; James Spates, "The Sociology of Values" 39)

⁷⁷ John Scott, *A Matter of Record* 30.

Table 3 Hacker manifestos

Computer scientists and Computer hobbyists	Underground hackers	FOSS developers	Hactivists	Makers
The Hacker Ethic (1984) ⁷⁸	The Conscience of a Hacker (1986) ⁷⁹	The GNU Manifesto (1985) ⁸⁴	A Cypherpunk's Manifesto (1993) ⁸⁹	The Maker's Bill of Rights (2006) ⁹⁴
	The Techno-Revolution (1986) ⁸⁰	The Cathedral and the Bazaar (1999) ⁸⁵	A Declaration of the Independence of Cyberspace (1996) ⁹⁰	The Cult of Done Manifesto (2009) ⁹⁵
	The Crypto Anarchist Manifesto (1992) ⁸¹	The dotCommunist Manifesto (2003) ⁸⁶	Guerilla Open Access Manifesto (2008) ⁹¹	Repair Manifesto (2009) ⁹⁶
		The Apache Way (2009) ⁸⁷		Self-Repair Manifesto (2010) ⁹⁷
		Open Hardware Constitution (2011) ⁸⁸	An Anonymous Manifesto (2011) ⁹²	The Hardware Hacker Manifesto (2010) ⁹⁸
			The Declaration of the Independence of the people of the Internet (2012) ⁹³	The User's Manifesto (2010) ⁹⁹
				A Kit Maker's Manifesto (2011) ¹⁰⁰
				The {Unspoken} Rules of Open Source Hardware (2012) ¹⁰¹
				The Fixer's Manifesto (2012)
				A Personal Design Manifesto (2013) ¹⁰²
				The MakerBot Way (2013) ¹⁰³
				This is the Maker Manifesto (2013) ¹⁰⁴
			The Maker Movement Manifesto (2014) ¹⁰⁵	
			10 Commandments of Making (2014) ¹⁰⁶	

Of the manifestos listed in Table 3, Steven Levy’s “The Hacker Ethic”,¹⁰⁷ the Mentor’s “The Conscience of a Hacker”,¹⁰⁸ and the Richard Stallman’s “The GNU Manifesto”¹⁰⁹ were selected for analysis because they are the most well known in the hacker community. These three texts have been repeatedly cited in other hacker writings and are often referred to or mentioned by all hacker types (including many makers and hacktivists) when they speak about or try to explain their norms and values. It is interesting to note that none of the three are explicitly entitled manifestos (although the Mentor’s piece is also popularly called “The Hacker Manifesto”). It bears repeating that, as long as a text has certain manifestary elements and characteristics, it is

⁷⁸ Steven Levy, *Hackers* 27.

⁷⁹ The Mentor, “The Conscience of a Hacker” Phrack <<http://phrack.org/issues/7/3.html>> accessed 28 April 2014.

⁸⁰ Doctor Crash, “The Techno-Revolution” Phrack <<http://phrack.org/issues/6/3.html>> accessed 4 July 2013.

⁸¹ Timothy C. May, “The Crypto-Anarchist Manifesto” <<http://www.activism.net/cyberpunk/crypto-anarchy.html>> accessed 27 May 2014.

⁸² Christian As. Kirtchev, “A Cyberpunk Manifesto” <http://project.cyberpunk.ru/idb/cyberpunk_manifesto.html> accessed 27 May 2014.

⁸³ McKenzie Wark, “A Hacker Manifesto” <http://subsol.c3.hu/subsol_2/contributors0/warktext.html> accessed 27 May 2014.

⁸⁴ Richard Stallman, “The GNU Manifesto” <<https://www.gnu.org/gnu/manifesto.html>> accessed 22 May 2014.

⁸⁵ Eric Raymond, *The Cathedral and the Bazaar*.

⁸⁶ Eben Moglen, “The dotCommunist Manifesto” <http://emoglen.law.columbia.edu/my_pubs/dcm.html> 23 February 2014.

⁸⁷ Shane Curcuro, “An Apache Way Primer” <<http://theapacheway.com/>> accessed 14 February 2013.

⁸⁸ “Open Hardware Constitution” <wiki.openhardware.org/Project:Constitution> accessed 12 October 2012.

⁸⁹ Eric Hughes, “A Cypherpunk’s Manifesto” <www2.eff.org/Privacy/Crypto/Crypto_misce/cyberpunk.manifesto> accessed 17 July 2013.

⁹⁰ John Perry Barlow, “A Declaration of the Independence of Cyberspace” <<https://projects.eff.org/~barlow/Declaration-Final.html>> accessed 27 May 2014.

⁹¹ Aaron Swartz, “Guerrilla Open Access Manifesto” <https://archive.org/stream/GuerrillaOpenAccessManifesto/Goamjuly2008_djvu.txt> accessed 1 February 2013.

⁹² Anonymous, “An Anonymous Manifesto” <anonnews.org/press/item/199/> accessed 17 July 2013.

⁹³ “The Declaration of the Independence of the people of the Internet” <http://files.gendo.nl/media/Pirate_declaration_of_Independence_2_printable.pdf> accessed 26 August 2013.

⁹⁴ Philip Torrone, “The Maker’s Bill of Rights” <<http://makezine.com/2006/12/01/the-makers-bill-of-rights/>> accessed 27 May 2014.

⁹⁵ Bre Pettis and Kio Stark, “The Cult of Done Manifesto” <<http://www.brepettis.com/blog/2009/3/3/the-cult-of-done-manifesto.html>> accessed 28 November 2012.

⁹⁶ Platform21, “Repair Manifesto” <www.platform21.nl/download/4375> accessed 28 November 2012.

⁸¹ Timothy C. May, “The Crypto-Anarchist Manifesto” <<http://www.activism.net/cyberpunk/crypto-anarchy.html>> accessed 27 May 2014.

⁹⁷ iFixit, “Self-Repair Manifesto” <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014.

⁹⁸ Cody Brocious, “The Hardware Hacker Manifesto” <daeken.com/the-hardware-hacker-manifesto> accessed 17 July 2013.

⁹⁹ Devin Coldewey, “The User’s Manifesto” <<http://techcrunch.com/2010/04/18/the-users-manifesto-in-defense-of-hacking-modding-and-jailbreaking/>> accessed 23 April 2014.

¹⁰⁰ Jake Spurlock, “A Kit Maker’s Manifesto” <<http://makezine.com/magazine/kitguide/maker-manifesto/>> accessed 17 July 2013.

¹⁰¹ Philip Torrone, “The {Unspoken} Rules of Open Source Hardware” <blog.makezine.com/2012/02/14/soapbox|the{unspoken}|rules|of|open|source|hardware/> accessed 5 October 2012.

¹⁰² Jan Borchers and Rene Bohne, “A Personal Design Manifesto” <fabworkshop.media.mit.edu/2013/04/09/a-personal-design-manifesto/> accessed 31 May 2013.

¹⁰³ MakerBot, “The MakerBot Way” <www.makerbot.com/blog/2013/06/14/the-makerbot-way/> accessed 21 June 2013.

¹⁰⁴ Maker Faire Africa, “This is the Maker Manifesto” <makerfaireafrica.com/maker-manifesto/> accessed 17 July 2013.

¹⁰⁵ Mark Hatch, *The Maker Movement Manifesto* 1-2.

¹⁰⁶ Adam Savage, “10 Commandments of Making” <<http://makezine.com/2014/05/19/adam-savages-10-commandments-of-making/>> accessed 3 June 2014.

¹⁰⁷ Steven Levy, *Hackers* 27.

¹⁰⁸ The Mentor, “The Conscience of a Hacker” (the Mentor’s real name is Loyd Blankenship).

¹⁰⁹ Richard Stallman, “The GNU Manifesto”.

deemed a manifesto.¹¹⁰ Two other manifestos, “An Anonymous Manifesto” and “This is the Maker Manifesto”, while not as widely known in the broader hacker community, have been included in the analysis because they are typical of the current crop of hacktivist and maker manifestos because they are written in a similar language, tone and style, embody a particular worldview, and express the same beliefs and concerns of hacktivists and makers, respectively.

3.3.2.1 The Hacker Ethic

Among hackers, Levy’s “The Hacker Ethic” is widely considered to be one of the founding declaration of some of the core elements and principles of hacker culture. It is important to point out though that “The Hacker Ethic” appears in Levy’s book *Hackers: Heroes of the Computer Revolution*, which is a non-scholarly book targeted to a mass audience. Levy is a well-respected writer and journalist who has written many books and articles about technology, but he is neither a hacker nor a social scientist. The research that he conducted for this book was also not expressly done pursuant to theories and methods of any academic discipline aside from journalism. However, there is still much value in Levy’s book as a source of data since it was based on over a hundred interviews with computer scientists and computer hobbyists.¹¹¹ Furthermore, “The Hacker Ethic” is particularly relevant because it is the first formal codification of the principles and philosophy of the first hacker generations. Prior to this, hacker culture and statements about its norms and values were not explicitly written down and were simply accepted and implicitly conformed to by hackers.¹¹² It is also worth noting that Levy wrote “The Hacker Ethic” during a period of crisis and change. As explained in Section 2.2.2.5, by the early 1980s, the originally free and open culture of hacking was giving

¹¹⁰ Galia Yanoshevsky, “The Decades of Writing on Manifesto” 262 and 265.

¹¹¹ Steven Levy, *Hackers* 479.

¹¹² Steven Levy, *Hackers* x and 27.

¹¹³ Steven Levy, *Hackers* ix; see Debora Halbert, “Discourses of Danger and the Computer Hacker”.

way to the increasing commercialization, proprietization and closure of computing. This was also a time when hackers were beginning to be vilified in and by the media, and prosecuted by authorities.¹¹³ It may be said that Levy was not just writing about, but also for and on behalf of the first generations of hackers. While this reveals an apparent partiality or bias that Levy has in favor of hackers, it is clear that he meant “The Hacker Ethic” and his entire book to be a wake-up call and an exhortation for people to recognize the important role that hackers play in society and to preserve the freedom, openness and dynamism of computer innovation.¹¹⁴ At time he wrote his book, Levy was not very optimistic about the original hacker culture’s chances of survival since he referred to Richard Stallman, who would become the founder of the free software movement, as “the last of the true hackers”.¹¹⁵

Despite the above limitations and qualifications, “The Hacker Ethic” remains a pertinent source of data for examining the norms and values of hackers. Many hackers and of all types, including the famous German hacker collective, the Chaos Computer Club, refer to and use “The Hacker Ethic” as their founding principles and guides for action.¹¹⁶ Despite being written by a person outside of their community, many hackers claim to subscribe to “The Hacker Ethic”. As Jordan and Taylor explain,

Rather than hackers themselves learning the tenets of the hacker ethic, as seminally defined by Steven Levy, they negotiate a common understanding of the meaning of hacking of which the hacker ethic provides a ready articulation. Many see the hacker ethic as a foundation of the hacker community.¹¹⁷

True to the manifesto genre, “The Hacker Ethic” is comprised of six tenets that are written in a hortatory and exaggerated style, tone

¹¹⁴ Steven Levy, *Hackers* x and 464.

¹¹⁵ Steven Levy, *Hackers* 437.

¹¹⁶ Chaos Computer Club, “hackerethics”.

¹¹⁷ Tim Jordan and Paul Taylor, “A sociology of hackers” 774-775.

and language:

Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!

All information should be free.

Mistrust Authority – Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.¹¹⁸

The above tenets are clearly normative in character and are statements about what hackers value. Using the values in Table 1.2, the first tenet (total and unlimited access to computers) involves values concerning openness, freedom of information, freedom of access, and personal growth. The second tenet (all information should be free) similarly affirms the importance of openness, freedom of information, freedom of access, and transparency to hackers. The values of individual autonomy and liberty and decentralization and self-governance are supported by the third tenet (mistrust authority). The fourth tenet (judgment based on actions and ability) clearly relates to equality and meritocracy and creativity and innovation. With regard to the fifth tenet (creation of art and beauty), the values of freedom of expression and creativity and innovation are specifically implicated. Finally, the sixth tenet (life improvement) clearly supports the value of personal growth.

¹¹⁸ Steven Levy, *Hackers* 28-34.

3.3.2.2 The Conscience of a Hacker

The Mentor's "The Conscience of a Hacker" is another manifesto document that has been highly influential in the hacker community.¹¹⁹ The piece was written by the Mentor in January 1986 after his arrest, and first appeared in the online hacker magazine Phrack later that year.¹²⁰ He was a member of the prominent American underground hacker group, Legion of Doom, and ran his own underground Bulletin Board System (BBS).¹²¹ Aside from being a hacker, he was also a writer and became managing editor at Steve Jackson Games, a role-playing and strategy game company that was raided by the authorities as part of the crackdown on underground hackers.¹²²

"The Conscience of a Hacker" has the hallmarks of a manifesto. It is made up of short paragraphs but the writing is very literary and poetic with its use of repetition and refrains (e.g., "Damn kid", "They're all alike", "you call us criminals"). It has a polemical and combative tone and uses aggressive and defiant language. To illustrate, the Mentor writes:

.... We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting

¹¹⁹ David Wall, *Cybercrime* 55.

¹²⁰ The Mentor, "The Conscience of a Hacker" <<http://phrack.org/issues/7/3.html>> accessed 28 April 2014.

¹²¹ Bruce Sterling, *The Hacker Crackdown* 89 (see Chapter 2 for more information about hackers and BBSes).

¹²² Bruce Sterling, *The Hacker Crackdown* 246 and 274; see "GURPS Cyberpunk" <<http://www.sigames.com/gurps/books/cyberpunk/>> (accessed 28 April 2014)

¹²³ The Mentor, "The Conscience of a Hacker" <<http://phrack.org/issues/7/3.html>> accessed 28 April 2014.

you, something that you will never forgive me for.¹²³

The words “we” and “us” (as opposed to the “you” or “they” of parents and authority figures) is used to refer to the community of underground hackers. The Mentor is decrying his and other hackers’ recent arrests and adamantly affirms the identity, norms and values of underground hackers, which he believes are diametrically opposed to the status quo, including the legal order. In this highly provocative and evocatively written piece, the Mentor makes normative and value-laden statements about what hackers consider important: curiosity (“My crime is that of curiosity”), equality and meritocracy (“We exist without skin color, without nationality, without religious bias”), freedom of access (“We make use of a service already existing without paying for what could be dirt-cheap if it wasn’t run by profiteering gluttons”), freedom of information (“We seek after knowledge”), individual autonomy and liberty (“We explore.... This is our world now”), creativity and innovation (“I found a computer. Wait a second, this is cool. It does what I want it to”), fun and play (“All he does is play games”), and personal growth (“a door opened to a world”).¹²⁴ He ends with the forceful and resolute lines, which signal the manifesto’s moment of action: “I am a hacker, and this is my manifesto. You may stop the individual, but you can’t stop us all... after all, we’re all alike”.¹²⁵ “The Conscience of a Hacker” is both a call for solidarity and a call to action among the underground hackers during a time when their group identity and personal security were being threatened by increasing criminal prosecution by law enforcement.

3.3.2.3 The GNU Manifesto

“The GNU Manifesto” was written and subsequently reworked by Richard Stallman during the early years of the GNU Project.¹²⁶

¹²⁴ The Mentor, “The Conscience of a Hacker” <<http://phrack.org/issues/7/3.html>> accessed 28 April 2014.

¹²⁵ The Mentor, “The Conscience of a Hacker” <<http://phrack.org/issues/7/3.html>> accessed 28 April 2014.

¹²⁶ Richard Stallman, “The GNU Manifesto”; see Chapter 2 for history and context.

The document does not merely explain the objectives and underlying philosophy of the GNU Project but, as a manifesto, it has the further aim of seeking out and inspiring kindred spirits to join the cause of free software and take immediate action.¹²⁷ Like “The Hacker Ethic”, it was written during a time of great crisis when the commercialization and the steadfast focus of treating software as exclusive property were undermining the original tenets of the hacker community. Stallman explains the problems that he and other hackers faced at the time:

I consider that the Golden Rule requires that if I like a program I must share it with other people who like it. Software sellers want to divide the users and conquer them, making each user agree not to share with others. I refuse to break solidarity with other users in this way. I cannot in good conscience sign a non-disclosure agreement or a software license agreement. For years I worked within the Artificial Intelligence Lab to resist such tendencies and other inhospitalities, but eventually they had gone too far: I could not remain in an institution where such things are done for me against my will.¹²⁸

This hortatory and oppositional style and tone is present throughout the text. Stallman for example speaks of how the GNU Project will allow him to “to continue to use computers without dishonor”.¹²⁹ While the manifesto is written in the first person, Stallman is actually writing to and speaking on behalf of the “We” of hackers and computer programmers who place great importance on sharing, collaboration and community building.¹³⁰

The manifesto’s main objective was to challenge the closed and proprietary approach to software development that was becoming ever more dominant, and to reinvigorate the culture of sharing and openness among hackers. As Stallman writes:

Many programmers are unhappy about the commercialization

¹²⁷ Richard Stallman, “The GNU Manifesto”.

¹²⁸ Richard Stallman, “The GNU Manifesto”.

¹²⁹ Richard Stallman, “The GNU Manifesto”.

¹³⁰ Richard Stallman, “The GNU Manifesto”.

of system software. It may enable them to make more money, but it requires them to feel in conflict with other programmers in general rather than feel as comrades. The fundamental act of friendship among programmers is the sharing of programs; marketing arrangements now typically used essentially forbid programmers to treat others as friends.¹³¹

However, unlike “The Hacker Ethic” and “The Conscience of a Hacker”, “The GNU Manifesto” has clear and definite program for radical action and social change. A major part of the plan involved building a “complete Unix-compatible software system” and “give it away free to everyone who can use it”.¹³² But instead of making the GNU Project a purely technical pursuit, “The GNU Manifesto” sought to promote an alternative and subversive approach to software development that ensured that the GNU Project remained free and open to all. The manifesto contains the beginning formulation of the idea of copyleft:

GNU is not in the public domain. Everyone will be permitted to modify and redistribute GNU, but no distributor will be allowed to restrict its further redistribution. That is to say, proprietary modifications will not be allowed. I want to make sure that all versions of GNU remain free.¹³³

The manifesto proposed a radical and powerful way to create and share computer code while remaining true to the values of the hacker community. “The GNU Manifesto” actualized the manifesto’s moment of action by asking other programmers to join the movement and produce free software.¹³⁴

“The GNU Manifesto” is suffused with statements about vital hacker norms and values. The values of openness, freedom of information, and freedom of access are supported by the norm of sharing

¹³¹ Richard Stallman, “The GNU Manifesto”.

¹³² Richard Stallman, “The GNU Manifesto”.

¹³³ Richard Stallman, “The GNU Manifesto”.

¹³⁴ Richard Stallman, “The GNU Manifesto”.

(“copying all or parts of a program is as natural to a programmer as breathing, and as productive. It ought to be as free”).¹³⁵ For Stallman, the free sharing of computer code is logical and desirable because it promotes the values of efficiency (“It means that much wasteful duplication of system programming effort will be avoided. This effort can go instead into advancing the state of art”), social development (“restricting their use of [a program] is destructive because the restrictions reduce the amount and the ways the program can be used. This reduces the amount of wealth that humanity derives from the program”), and individual autonomy and liberty (“Complete system sources will be available to everyone. As a result, a user who needs changes in the system will always be free to make them himself”).¹³⁶ The manifesto also upholds the importance of creativity and innovation (“If anything deserves a reward, it is social contribution. Creativity can be a social contribution, but only in so far as society is free to use the results”).¹³⁷ In his defense of the free software development model, Stallman mentions how hackers prize the values of personal growth and fun and play (“[Programmers] got many kinds of nonmonetary rewards: fame and appreciation, for example. And creativity is also fun, a reward in itself”).¹³⁸

3.3.2.4 An Anonymous Manifesto

Hacktivist manifestos are closely related to and mainly build on the earlier writings of underground hackers like the Mentor. While no hacktivist manifesto has yet been as popular, influential or canonical as the three documents discussed above, “An Anonymous Manifesto” is a typical example of hacktivists’ writings about their goals and concerns.¹³⁹ This document was written by members of the hacktivist

¹³⁵ Richard Stallman, “The GNU Manifesto”.

¹³⁶ Richard Stallman, “The GNU Manifesto”.

¹³⁷ Richard Stallman, “The GNU Manifesto”.

¹³⁸ Richard Stallman, “The GNU Manifesto”.

¹³⁹ Anonymous, “An Anonymous Manifesto”.

group Anonymous, which is composed of technical and non-technical persons.¹⁴⁰ Anonymous claims to have “no leaders, no hierarchical structure, nor any geographical epicenter”¹⁴¹, and, typical of hacker groups, has fluid membership and a high turnover rate.

“An Anonymous Manifesto” was written in early 2011 when the group was engaging in bold acts of hacktivism, including carrying out distributed denial-of-service (DDoS) attacks, against companies and governments around the world that they believe were acting unfairly and unjustly.¹⁴² Since Anonymous was being equally praised and vilified in the media for their actions, this manifesto was an attempt by a few members of the group to formally set down in writing their aims and philosophy for their own as well as others’ edification. As they say at the beginning of the manifesto: “Recently there has been some confusion as to our identities and our motives. Some of us would like to try and clear a few things up”.¹⁴³

“An Anonymous Manifesto” is what people normally expect a manifesto to be. First, the title declares that it is so. Second, it is a brief text that contains numbered theses of the group’s principles. Third, its language and tone are hortatory and defiant. Additionally, the text is publicly asserted and signed by a collective “We”. The manifesto is meant to be a critical discursive attack on dominant and powerful institutions and organizations and aims to stand up to them. The manifesto moment takes place when the reader is enjoined: “Becoming Anonymous is simple. Just take action”.¹⁴⁴ Like “The Conscience of a Hacker”, it similarly ends in an ominous way:

We are Anonymous.

We are Legion.

¹⁴⁰ E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”; see Parmy Olson, *We Are Anonymous*.

¹⁴¹ E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”.

¹⁴² E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”.

¹⁴³ Anonymous, “An Anonymous Manifesto”.

¹⁴⁴ Anonymous, “An Anonymous Manifesto”.

We do not Forget.

We do not Forgive.

Expect Us.¹⁴⁵

As a formal declaration of their goals and beliefs, the manifesto contains explicit and unequivocal statements about their norms and values. Members of Anonymous clearly value anonymity (“Anonymous is everyone. Anonymous is no one. Anonymous exists only as an idea. You also can be Anonymous.”),¹⁴⁶ but they also want to expressly “promote an open, fair, transparent, accountable and just global society”.¹⁴⁷ In many statements in the text, the following values are plainly manifest: openness (“promote an open... global society”), freedom of information and freedom of access (“a society must be allowed to share information unrestricted and uncensored”), individual autonomy and liberty (“uphold the rights and liberties of its citizens”), privacy (“No citizen should be denied protection against any undue interference to his/her privacy”), transparency (“maintain an open and transparent society”), creativity and innovation (“to maintain cultural and technological evolution”), and decentralization and self-governance (“Citizens must be allowed to organize their own institutions without being harassed by existing institutions privileged by greater resources, influence and power”).¹⁴⁸

3.3.2.5 This is the Maker Manifesto

It is interesting to note that the interest in the manifesto genre has not waned among makers. In fact, as shown in Table 3, there is a glut of manifestos for and about the maker movement. “This is the Maker Manifesto” is typical of the manifestos written by makers. Maker

¹⁴⁵ Anonymous, “An Anonymous Manifesto”.

¹⁴⁶ Anonymous, “An Anonymous Manifesto”.

¹⁴⁷ Anonymous, “An Anonymous Manifesto”.

¹⁴⁸ Anonymous, “An Anonymous Manifesto”.

manifestos normally consist of a single page containing a numbered list of the key principles and statement of and about a group that has been graphically designed and laid out to look visually interesting or eye-catching. This is unlike the manifestos of previous hacker generations that were merely printed or laid out using simple texts without any thought about design. In addition, maker manifestos are generally less radical and aggressive in both their outlook and proposed actions. They are written primarily for the members of their community and deal with internal matters and concerns.

“This is the Maker Manifesto” was written on the occasion of a Maker Faire in Africa. Compared to the “An Anonymous Manifesto”, the words used are not polemical, but they remain hortatory and aspirational because the aim is to produce personal and social development through direct and immediate action (“If you want something you’ve never had, then you’ve got to do something you’ve never done”).¹⁴⁹ It is written for and by the “We”, makers in Africa (“We will remake Africa with our own hands”).¹⁵⁰

The manifesto plainly seeks to achieve or promote values relating to: freedom of access (“We will share what we make”), creativity and innovation (“We will see challenges as opportunities to invent”), individual autonomy and liberty (“We will be responsible for acting on our own ideas”), and community development (“We will share what we make, and help each other make what we share”).¹⁵¹ Like “The Hacker Ethic”, it champions the “Hands-On Imperative” (“We will remake Africa with our own hands” and “We will be obsessed with improving things, whether just a little or a lot”).¹⁵² The document further underscores the important activities of sharing and working together

¹⁴⁹ Maker Faire Africa, “This is the Maker Manifesto”.

¹⁵⁰ Maker Faire Africa, “This is the Maker Manifesto”.

¹⁵¹ Maker Faire Africa, “This is the Maker Manifesto”.

¹⁵² Maker Faire Africa, “This is the Maker Manifesto”.

¹⁵³ Maker Faire Africa, “This is the Maker Manifesto”.

(“We will forge collaborations”).¹⁵³ It powerfully hammers home these values through repetition by starting all declarations with the phrase “We will”.¹⁵⁴ The manifesto’s moment of action takes place when the forward-looking and repeated phrase “We will” is set in motion by the title “This is the Maker Manifesto”,¹⁵⁵ which declares that the time to act is now.

All in all, hacker manifestos exhibit the norms and values of different types of hackers and hacker culture as a whole. As expressions of their beliefs and aspirations, manifestos are a rich source for examining their norms and values. Furthermore, for hackers themselves, manifestos symbolize and are touchstones of their identity and culture. These writings play a key role in the community formation and socialization of hackers. Manifestos like “The Hacker Ethic” and “The GNU Manifesto” are texts that hackers actually live by and they serve as constant calls to action.

3.4 Norms and values of makers and hacktivists

Based on my interviews with makers, hacktivists and other members of the hacker community and fieldwork at hacker events and hackerspaces in the Netherlands, I was able to observe and gather data about all of the hacker values mentioned in Table 1.2: anonymity, community development, consensus, creativity and innovation, curiosity, efficiency, equality and meritocracy, freedom of access, freedom of expression, freedom of information, fun and play, decentralization and self-governance, individual autonomy and liberty, openness, personal growth, privacy, security, social development, and transparency. But some norms and values stood out more than others. Specifically during interviews, when I asked hackers to prioritize which values were most important to or for them, the five that were most selected in aggregate were: creativity and innovation, curiosity, individual autonomy

¹⁵⁴ Maker Faire Africa, “This is the Maker Manifesto”.

and liberty, community development, and social development.

While there is a general commonality in what hackers value most, there is some variance among the different types of hackers that I met. For makers, aside from creativity and innovation and individual autonomy and liberty, they also prize the values of openness and transparency. In comparison, hacktivists, in addition to individual autonomy and liberty and community and social development, consider curiosity and equality and meritocracy to be very significant. I also spoke to a few ethical hackers during my research and for them, besides creativity and innovation, curiosity, and community and social development, they also place great store in the value of security.

3.4.1 CREATIVITY AND INNOVATION

It comes as no surprise that creativity and innovation is considered one of the most significant values for hackers. This is expected given that innovation is an essential element of a hack and “hacking in itself is just creatively using technology”.¹⁵⁶ The makers, hacktivists and other hackers I spoke to generally define themselves and their activities in relation to technological creativity and innovation. As Maker K explains, “so in that sense I am a hacker because I’m creative. I like to know how to change [things]. I really like to know how things work”.¹⁵⁷ Maker F says, “I’m a maker in a sense that I’m a creative person. So I’m always creating things. I’m making things”.¹⁵⁸ Some consider “[m]aking, creating something” as “a valuable experience in its own right”.¹⁵⁹ Hacktivist D sees “hackers as people who reuse technology in ways not imagined by the people who bought the thing or the program or

¹⁵⁵ Maker Faire Africa, “This is the Maker Manifesto”.

¹⁵⁶ Interview with Maker J.

¹⁵⁷ Interview with Maker K.

¹⁵⁸ Interview with Maker F.

¹⁵⁹ OHM2013, “Make”.

¹⁶⁰ Interview with Hacktivist D.

¹⁶¹ Interview with Hacktivist B.

technology”.¹⁶⁰ Whether for makers or hacktivists, hacking is about having a “creative, critical approach to technology”.¹⁶¹

Based on my interviews and interactions with members of the Dutch hacker community, creativity and innovation is prized more by makers than hacktivists. Makers are especially passionate about building or doing new things with technology, whereas hacktivists are more inclined to use technology as means for achieving socio-political goals. For makers, the great appeal of hacking is that “you can take something and reorganize or reshuffle it to make something completely different”.¹⁶² According to Maker C, “This inner thing, that maker spirit, this whole idea of just doing stuff, that’s how we learn”.¹⁶³ Some describe it as a “mentality and attitude... finding where you can stretch a system to do new things”.¹⁶⁴ Maker A even believes “it’s in my blood” to build and create things.¹⁶⁵

The value of creativity and innovation though does not simply remain a personal or individual goal but is shared and pursued by the entire group or community. In hackerspaces, for instance, “everybody is searching for smart solutions, original combinations and cheap solutions”¹⁶⁶ and “the typical project that we have are for fun, and to learn and to do cool stuff”.¹⁶⁷ Makers subscribe to the do-it-yourself mentality and would rather build something than buy it. People who can build their own 3D printers, CNC machines, laser cutters and laser light projectors from scratch are held in high esteem in the community, especially if they were able make them better and cheaper than commercially available models. But for makers, it is not enough to have produced these machines. They consider it essential to share what they learned with others. There is a clear understanding among makers that the ability to create is intimately connected to each per-

¹⁶² Interview with Maker K.

¹⁶³ Interview with Maker C.

¹⁶⁴ Interview with Hactivist A.

¹⁶⁵ Interview with Maker A.

¹⁶⁶ Interview with Maker B.

¹⁶⁷ Interview with Maker D.

son's propensity to share and learn from each other, which are both common acts of hacking. As Maker I states, "having discovered that there is this dynamic where people build on top of each other, and you really want to also be part of that, and you want more people to become part of that".¹⁶⁸ Part of the allure of working together in a hackerspace is that "we build very cool equipment... that we are proud about, and everybody can join".¹⁶⁹ The value of creativity and innovation has a distinct social dimension and purpose, which is why, for Maker C, "I want to let anyone make anything, or do whatever I can to do that, to bring that about".¹⁷⁰ In fact, the motto of one hackerspace is "to creatively use technology to improve the world".¹⁷¹

This imperative to create and be creative with technology seems to be hardwired to the very constitution of makers, hacktivists and other types of hackers. As Hactivist C exclaims, "There's no in-between. Either I go forward or stop and start doing something else".¹⁷² There is an unmistakable impetus to innovate. As Maker K reflects, "Yeah I suppose that's really what motivates me. I just think, can we do that, how better can we do it".¹⁷³ The need to be creative and innovative can also be quite an obsession for some. As recounted by Ethical Hacker A,¹⁷⁴ "For me it's really difficult to the same trick over and over again. I don't like that. So, on the other side of the spectrum, what I do like is things that are different each and every time".¹⁷⁵ The comparison between hackers, artists and other creative types is unavoidable since they can all be described as "creative people with a lot of passion, doing a lot of good work".¹⁷⁶ It is worth noting that there are a number of artists and designers who are part of or have close ties to the hacker

¹⁶⁸ Interview with Maker I.

¹⁶⁹ Interview with Maker D.

¹⁷⁰ Interview with Maker C.

¹⁷¹ Interview.

¹⁷² Interview with Hactivist C.

¹⁷³ Interview with Maker K.

¹⁷⁴ An ethical hacker, also known as a white hat hacker, is a person who breaks into a computer or information system to "find security flaws" and improve its security (Cassandra Kirsch, "The Grey Hat Hacker" 386; see also Ronald Raether Jr., "Data Security and Ethical Hacking" 55).

¹⁷⁵ Interview with Ethical Hacker A.

¹⁷⁶ Interview with Maker B; see also Paul Graham, *Hackers & Painters*.

community and art installations figure prominently at hacker camps and events.¹⁷⁷

3.4.2 CURIOSITY

Creativity and innovation are intimately related to another value – curiosity. These values seem to naturally go hand-in-hand and statements made by hackers about curiosity generally relate to creativity and innovation, and vice versa. The close connection between curiosity and creativity and innovation is evident as well to the hackers I spoke to. Ethical Hacker B says, “in a sense, if I look at creativity and innovation, I think that also covers curiosity”.¹⁷⁸ Another hacker concurs, “so actually creativity and innovation, curiosity is similar”.¹⁷⁹ What differentiates curiosity from creativity and innovation is that the former is an instrumental value for hackers to explore and learn how things work, while the latter is concerned with a terminal goal of producing something new or different.

Even though hackers seem to prioritize creativity and innovation slightly more than curiosity, the latter remains an essential value that is commonly shared among the makers, hacktivists and other hackers that I spoke to. What makes curiosity so significant to hackers is that it “necessarily precedes” and is “a necessary condition” for hacking.¹⁸⁰ For many of the makers and hacktivists that I met, curiosity was one of the main reasons or motivations why they pursued or engaged in hacker projects and activities.¹⁸¹ According to Hactivist E, “curiosity is fulfilled throughout all of these activities”.¹⁸² Maker A says that curiosity “usually starts my thinking process”,¹⁸³ and, for Maker E,

¹⁷⁷ See OHM2013, “Program”; see OHM2013, “Call for Participation”.

¹⁷⁸ Interview with Ethical Hacker B.

¹⁷⁹ Interview with Ethical Hacker A.

¹⁸⁰ Interview with Hactivist E.

¹⁸¹ Interview with Maker J; Interview with Hactivist B.

¹⁸² Interview with Hactivist E.

¹⁸³ Interview with Maker A.

¹⁸⁴ Interview with Maker E.

“it’s always curiosity that drives the next thing”.¹⁸⁴ Hacking is propelled by a natural curiosity to understand how technology works and how to make it better.¹⁸⁵ “I’m curious about how it works, how I can make something work better, how I can make it smaller, bigger”, explains Maker A.¹⁸⁶ Maker K describes the thinking and creative process, “I just like seeing the what if. That’s I suppose what really motivates me. What if, could we do that? Then I go off and I try it”.¹⁸⁷ Curiosity thus leads to various paths to explore and learn about technology, which are common acts of hacking, “I really like to experiment with a lot of stuff”, says Maker A.¹⁸⁸ This desire to experiment is also carried over in hacker camps where hackers “expect some interesting new discoveries and observations about the technology we see around us in our everyday lives”.¹⁸⁹

One interesting aspect of curiosity is that it includes a sense of play and a bit of innocent mischief. Hackers explain the reason why they hold outdoor hacker camps, “Because we can! And fun. Definitely fun”.¹⁹⁰ Being curious about technology normally involves “playing, having fun and discovering stuff that wasn’t there before”.¹⁹¹ According to Maker F, “I always like things I don’t know and which tickles” my interest.¹⁹² For the hackers I met, it seems curiosity is an imperative that must be acted on. As Hactivist E explains, “I was simply too curious and the outcomes of my online adventures were simply too rewarding”.¹⁹³ When posed with the challenge of “Can you do this? Can you print this?”, Maker K’s recounts, “I go, ok I don’t know, let’s find out”.¹⁹⁴ Following one’s curiosity admittedly involves not just creative but also destructive activities. While working on a project, it is some-

¹⁸⁵ Interview with Hactivist B.

¹⁸⁷ Interview with Maker A.

¹⁸⁷ Interview with Maker K.

¹⁸⁸ Interview with Maker A.

¹⁸⁹ OHM2013, “Press release”.

¹⁹⁰ OHM2013, “FAQ”.

¹⁹¹ Interview with Hactivist D.

¹⁹² Interview with Maker F.

¹⁹³ Interview with Hactivist E.

¹⁹⁴ Interview with Maker K.

times necessary to break things. As Ethical Hacker B recounts, “we don’t really know how it works, and so maybe could you look to see if you can try to mangle with it”.¹⁹⁵ Most hackers will “try to find a hole, break it open as far as possible so they can get in”.¹⁹⁶ However, it is important to point out that, as Ethical Hacker B states, “I never really wanted to abuse it, but just to know how the system works”.¹⁹⁷ There is no malicious intent to cause damage. Of course, there is the possibility that hackers may accidentally cause damage to systems. In these cases, they will endeavor to minimize or fix the accidental or incidental damage they caused. Furthermore, while curiosity naturally involves playfulness, it is also a serious matter. As Hactivist B explains, curiosity is “a mindset in which we relate to the rest of the world without accepting the usual understanding of it”.¹⁹⁸ It provides “a wider view upon the meaning of the technologies that we live with”.¹⁹⁹ Makers and hactivists seek to “apply their critical curiosity and creativity to bring about methods to cope with the upcoming changes” in society.²⁰⁰

3.4.3 INDIVIDUAL AUTONOMY AND LIBERTY

For the makers and hactivists I spoke with, being creative, innovative or curious would not be possible in the absence of the requisite value of individual autonomy and liberty. Both makers and hactivists regard this value as extremely important because it is similarly a means to achieve other values as well as a goal in its own right. Liberty of choice and action is deemed essential to hacking since it would be impossible to engage in any or all of the common acts of hacking (explore, break, learn, create, share and secure) in the absence of this value. According to Maker E, “For us, it has a lot of advantages

¹⁹⁵ Interview with Ethical Hacker B.

¹⁹⁶ Interview with Maker A.

¹⁹⁷ Interview with Ethical Hacker B

¹⁹⁸ Interview with Hactivist B.

¹⁹⁹ Interview with Hactivist B.

²⁰⁰ OHM2013, “Call for Participation”.

²⁰¹ Interview with Maker E.

that we dictate our own path. We have nobody to answer to”.²⁰¹ Maker L exhorts, “Give people more freedom because with all those things that’s not possible. You have to do [this], you have to do that. You sometimes feel constrained in doing things. You’re less free”.²⁰² Maker F explains the relationship between individual autonomy and liberty to creativity and innovation: “Because only if you don’t have boundaries and it feels like you could do whatever you want, you could be on a higher level”.²⁰³ As Maker B succinctly puts it, “hackers are the most autonomous and creative individual people in the IT sector”,²⁰⁴ and, as such, it is commonly believed that having greater autonomy leads to more creativity.

An interesting revelation though that came up during my interviews and conversations with hackers is that despite being so technically minded and focused, they see the importance of freedom and autonomy not just with but also from technology. They are very much aware of “the danger of getting too dependent on systems and on centralized information dominance”, and that “we need to always be able to have our individual responsibility and freedom to choose”.²⁰⁵ They caution that “[b]lind faith in ICT in particular leads to erosion of democratic principles and human rights”.²⁰⁶ For Hacktivist E, “individuals should not be unreasonably forced [to use] systems, especially when those systems contradict the interests of individuals”.²⁰⁷ Some hackers would like “to take the technical expertise of the hacking scene out of its isolation to place it within the broader perspective of the societal structures it shapes and is part of”.²⁰⁸ As Maker I reflects, “I think the beauty of hacking is that it balances out a little bit the concentration or asymmetry of power”, whether it be political, technological or legal.

²⁰² Interview with Maker L.

²⁰³ Interview with Maker F.

²⁰⁴ Interview with Maker B.

²⁰⁵ Interview with Maker B.

²⁰⁶ OHM2013, “Call for Participation”.

²⁰⁷ Interview with Hacktivist E.

²⁰⁸ Interference, “Calling for Papers” <<http://interference.io/cfp.php>> accessed on 6 May 2014.

²⁰⁹ Interview with Maker I.

²⁰⁹ Many hackers I met believe that they can change the world and make it better through their hacking projects and activities.

Whether as individuals or as groups, hackers are undoubtedly very autonomous, independent and self-directed.²¹⁰ At hacker camps, people would typically spend long periods transfixed and hacking away at their own computers seemingly oblivious to everyone beside or near them. The phenomenon of being “alone together” is common too among hackers.²¹¹ According to Maker D, most people “like to do their own projects”.²¹² Even in the communal setting of a hackerspace, “most projects are done by one person”, although “people hope that other people will help or do something similar”.²¹³ Maker D explains why individual liberty and autonomy is highly prized among them, “If you build software on your own, you can decide how to do it yourself. That’s a good thing”.²¹⁴ For Hactivist E, “autonomy also includes deciding how the equipment you buy works: the ‘freedom to tinker’ allows the pursuit of hacker values; for instance to improve its features, to disable limitations that prevent sharing and fair use, or to make it more secure and less privacy-invasive”.²¹⁵ Of course, for some hactivists, too much autonomy can also be an issue since “we run up into the fact that we are all sort of quite anarcho-communist people that do not listen to each other”.²¹⁶

3.4.4 COMMUNITY DEVELOPMENT

Despite the strong emphasis on individual autonomy and liberty, makers and hactivists alike see the importance of building and being active in their communities. Hackers in the Netherlands even

²¹⁰ Interview with Maker I.

²¹¹ See Sherry Turkle, *Alone Together*.

²¹² Interview with Maker D.

²¹³ Interview with Maker G.

²¹⁴ Interview with Maker D.

²¹⁵ Interview with Hactivist E.

²¹⁶ Interview with Hactivist C.

formed an umbrella group of hackerspaces and hacker organizations in the belief that “Together we are stronger than alone”.²¹⁷ Dutch hackerspaces are on friendly terms with one another and they try to assist each other by giving “tips and tricks or experiences in setting up and keeping alive a hackerspace or event”.²¹⁸ They also use the regular hacker camps and events to meet, catch up, share knowledge and ideas and collaborate on projects. Many hackers that I met at these hacker camps initially appeared shy and introverted, but they were actually quite friendly and sociable with and among other hackers. They all knew each other. In the evenings, hacker camps had a party club vibe where people would hang out in small groups, chat, drink beer and Club-Mate, tell stories, joke around and have fun. The atmosphere was lively and upbeat but never rowdy. While it is true that hackers like their independence, hacker camps and other community events are important shared experiences for them.²¹⁹ Many hackers I spoke to were excited about an upcoming hacker camp and waxed lyrical about previous hacker camps they had been to. Some people wore t-shirts from past hacker camps they attended. There was a strong spirit of community and volunteerism at these camps. “[E]very visitor is both participant and volunteer” and everyone is expected to pitch in and actively take part.²²⁰ The entire camp was community-driven and organized and run by volunteers. Everyone was counted on to lend a hand: lay down power and internet cables across the camp grounds, build walkways, put up tents, move and set up equipment, man the entrance, drive the shuttle vans, cook food, pick up refuse, fix clogged toilets and showers, and give talks and workshops to others.²²¹ Camp wristbands and t-shirts prominently bear the word “crew” to remind everyone to help out since this is their camp.

²¹⁷ Hackerspaces.nl <<http://hackers.nl>> accessed on 12 November 2015; see also Hackerspace Open Day <<https://revspace.nl/HackerspaceDagEn2012>> accessed on 27 March 2013.

²¹⁸ Hackerspaces.nl <<http://hackers.nl>> accessed on 12 November 2015.

²¹⁹ See Gabriella Coleman, “The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld” 65.

²²⁰ OHM2013, “Press release”.

²²¹ See OHM2013, “FAQ”; see OHM2013, “Press release”.

This community spirit is quite useful as well when it comes to hackers' technical projects and activities. To learn how things work or to create something new are integral aspects and goals of hacking. But for the makers and hacktivists I spoke to, these are not enough. For them it is important as well to work together and share what they learned or created with others. At camps, for example, people taught each other how to mine for bitcoins, splice fiber optic cables and run a Tor server. They understand that sharing is essential in promoting not only creativity and innovation but also community development. There is a palpable communitarian ethos within the hacker community especially among makers. Building and having a sense of community is crucial, for instance, when setting up a hackerspace. As Maker B explains, hackerspaces are "a common place to connect to each other" and, like hacker camps and conferences, they act like a "kind of the physical touchdown" for the hacker community.²²² For Maker E, a hackerspace is "a community project so the word community obviously already reverberates through everything we do".²²³ Makers have varied reasons or motivations for going to hackerspaces, but many of them join "for the community mostly".²²⁴ They can quite easily work on their projects alone at home but makers who frequent hackerspaces "want to share and collaborate".²²⁵ They view hackerspaces as "just a big place where everybody can come together and work and hang out, drink a cup of coffee but also find cutting edge technology".²²⁶ While makers obviously go to hackerspaces to work on technical projects, ultimately, "it's about the people".²²⁷ For them a hackerspace "is not about the machines. It's about the facility. It's about the place where people come together."²²⁸ Because of this, "at the same time as we are

²²² Interview with Maker B.

²²³ Interview with Maker E.

²²⁴ Interview with Maker G.

²²⁵ Interview with Maker B.

²²⁶ Interview with Maker E.

²²⁷ Interview with Maker E.

²²⁸ Interview with Maker E.

trying to facilitate a group or a community feel, we also want to empower everybody individually and make them grow”, relates Maker E. Maker D further elaborates, “we want to build on these people so they can become better hackers, technologists, and build something with the space”.²²⁹

Like the computer hobbyists who started the PC revolution, collaborating with others makes perfect sense for makers and hacktivists alike. For them, it is a very logical and practical decision since working together is more effective and produces better results. According to Hactivist C, in order to have a greater impact, “you always have then to talk to others and put yourself into a team”.²³⁰ When dealing with technical or social issues, people at hackerspaces or hacker events have the “urge to meet with other people and talk about it and also to address certain topics”.²³¹ According to Maker B, “it’s inherent in the set up of an open space where everyone is welcome and thinking and working on these issues”.²³² The advantage of sharing is that people can “brainstorm about what they’re thinking about or just to chat. In that way you can really make a really nice community that helps each other”.²³³ It is common practice for makers to show “what you do, what’s available, learning [from] people, and hope other people can use your ideas. So it’s not only for you but everybody can use it”.²³⁴

Sharing and collaboration also produce a virtuous cycle where people are so “enthusiastic, so into what they are creating, what they are making, and they want to share it”.²³⁵ It is a common experience among makers that “people are willing to share their ideas with us because we also share with them, and we start by sharing with them”.²³⁶

²²⁹ Interview with Maker D.

²³⁰ Interview with Hactivist C.

²³¹ Interview with Maker B.

²³² Interview with Maker B.

²³³ Interview with Maker A.

²³⁴ Interview with Maker L.

²³⁵ Interview with Maker A.

²³⁶ Interview with Maker I.

The projects they work on do not remain individual technical pursuits, because, according to Maker I, “helping each other out, that’s also a part of it”.²³⁷ Like the FOSS developers who champion the benefits of technologies and systems that are free and open, Maker A believes that “if we just share everything we do and want, we get a whole lot more positive world than we are in now”.²³⁸ Makers understand that “technology is a really powerful thing, and by sharing those improvements you build on top of each other. You are lowering barriers”.²³⁹ According to Maker I, “I really like the fact that we’ve done a few things together that many more people started believing in and taking up and also contributing to”.²⁴⁰ Maker L agrees, “I think that is one of the most important things within hacking because if you are open, people can learn from you, you can learn from other people”.²⁴¹ Community development is thus a necessary corollary to individual autonomy and liberty because “it’s very difficult to do this by yourself. If everybody would do it by yourself, everyone will fail”.²⁴²

3.4.5 SOCIAL DEVELOPMENT

Intimately related to and following closely from community development is the value of social development. The hackers I met are not simply content with building their communities and learning how the world works. As with their approach to any technology, makers and most especially hacktivists also want to change, improve and make the world better. They genuinely want to understand “how we can change things and how can we make things better”.²⁴³ Hacktivist D explains the relationship between community development, social development and individual autonomy and liberty: “Having a healthy community

²³⁷ Interview with Maker I.

²³⁸ Interview with Maker A.

²³⁹ Interview with Maker I.

²⁴⁰ Interview with Maker I.

²⁴¹ Interview with Maker L.

²⁴² Interview with Maker D.

²⁴³ OHM2013, “Observe”.

and social development depends on people having enough individual autonomy and liberty to inform themselves and to be like a member of society or a member of the community”.²⁴⁴ Which is why when hackers organized workshops targeted to the general public to teach people how to use computers and other technologies more safely and securely, “we very explicitly don’t want people to come over, hand over their laptops and we install stuff for you and give it back.”²⁴⁵ According to a hacker, they “want to help and teach people but not do things for them”.²⁴⁶ For instance, hackers freely and voluntarily offered their knowledge and skills and took an active role in helping local councils develop a digital fabrication lab or convert a bus into a mobile hacking space to service their local communities. Dutch hackerspaces also hold an annual “Hackerspace Open Day” where they give the public a behind-the-scenes tour of their spaces and offer workshops and hands-on training on soldering, laser cutting and building devices with Arduino.²⁴⁷

There is a notable dynamic among the makers and hacktivists that I observed. While they value their personal liberty and autonomy from external controls and restraints, at the same time, they are equally aware that they are part of a wider community and they are keen on using their freedoms for the benefit of others and society as a whole. They understand that it is necessary to “balance individual liberties with sort of broader social needs or with broader social systems”.²⁴⁸ As Maker I relays, we “really feel like we’re part of the bigger community” than just the hacker community.²⁴⁹ Hackers may place great importance on the individual and their individuality, but because of their social goals and beliefs, they are far from being self-centered or individualistic.

²⁴⁴ Interview with Hactivist D.

²⁴⁵ Interview.

²⁴⁶ Interview.

²⁴⁷ Hackerspace Open Day <<https://revspace.nl/HackerspaceDagEn2012>> accessed on 27 March 2013.

²⁴⁸ Interview with Hactivist A.

²⁴⁹ Interview with Maker I.

Makers and hacktivists are cognizant of their social responsibility. They have “a feeling of responsibility for educating and protecting society”.²⁵⁰ As Maker D relates, “It’s good to do stuff for your own technology but we forget too much that there’s also a lot of work to do on improving this society”.²⁵¹ They see the imperative “to steer those developments into directions that have a collective good”.²⁵² For the makers that I met, 3D printing is about both technical and social change. Maker C explains, “I see the skill set of making and the skill set of 3D printing can lead to the fact that people can make anything they want and improve their lives”.²⁵³ Maker C continues, “That’s why I’m so fascinated with 3D printing. The idea is these machines can help together with a bunch of other technologies. For me these things are important”.²⁵⁴ Maker I agrees, “I think we can really change things and allow other people to also create change” with 3D printers.²⁵⁵ Maker I reflects on the role of technology in producing social change: “In a way, we’re not creating the major change but we’re creating a platform for change.... I like creating infrastructure because that can create a bigger effect”.²⁵⁶

Hacking is often thought of as being a completely technical pursuit. But for the makers and hacktivists that I got to know, they recognize the social dimensions and obligations of hacking. This is especially true since “society is more and more dependent on technology”.²⁵⁷ As Hactivist B states, “any interaction with technology at some point does affect society in a way that goes far beyond the manufacturing of an object or artifact”.²⁵⁸ Maker I concurs, “There’s so much technology changing society and if... we start thinking about this technology in

²⁵⁰ OHM2013, “Hack”.

²⁵¹ Interview with Maker D.

²⁵² Interview with Hactivist B.

²⁵³ Interview with Maker C.

²⁵⁴ Interview with Maker C.

²⁵⁵ Interview with Maker I.

²⁵⁶ Interview with Maker I.

²⁵⁷ OHM2013, “Call for Participation”.

²⁵⁸ Interview with Hactivist B.

a different way and by hacking” there can be a “macro effect”.²⁵⁹ For Maker D as well, “I always am aware that I do it for people and try to [help] people to become better in what they do”.²⁶⁰ Maker D continues, “Sharing information, building a platform for people to improve the society.... We want to become great people. That’s more important than building one great product”.²⁶¹ Makers and hacktivists believe that they have an important social role to play and having a “network of hackers is important because it’s a kind of a backbone for society” that is becoming increasingly technological and ever more connected.²⁶² They maintain that “[s]ociety increasingly depends on hackers to act as its conscience on these matters”.²⁶³

3.4.6 OTHER PROMINENT NORMS AND VALUES

Aside from the above five values that the makers and hacktivists I spoke to consider to be the most significant, based on my coding and analysis of interviews and other empirical data, there were other values that were particularly notable, namely: openness, freedom of access, transparency, security, and privacy. These values were especially prominent during my discussions with hackers about controversial topics such as the high profile hacking of electronic voting machines and the Dutch national public transport card (the OV-chipcard).

3.4.6.1 Openness and freedom of access

Openness has always been a central value for hackers.²⁶⁴ As discussed at length in Chapter 2, openness was a motive principle for previous hacker generations like computer hobbyists and FOSS developers, and the same is true for makers and hacktivists. Openness is a requisite to perform any and all of the common acts of hacking:

²⁵⁹ Interview with Maker I.

²⁶⁰ Interview with Maker D.

²⁶¹ Interview with Maker D.

²⁶² Interview with Maker B.

²⁶³ OHM2013, “Call for Participation”.

explore, break, learn, create, share and secure. Makers especially value openness. “I think being open to the world with the things you do is very important”, explains Maker L, “What for me is important in hacking is if it’s open so everybody can use it”.²⁶⁵ The ethos of openness extends not just to their technologies and technical activities, but also to their social relations and how they deal with others. “Being open” is fundamental “so everybody can get connected to each other”.²⁶⁶ Maker F recounts, “because we are so open, I think most people we work with, it’s a common thing to do. Everybody likes each other”.²⁶⁷ Maker E similarly reflects, “It is amazing to me that if you are so open and you share everything and then other people start doing that too”.²⁶⁸ Openness thus plays a crucial role in community building. This is especially true in hackerspaces where, according to Maker E, “we try to be as open as possible. We don’t want to set boundaries”.²⁶⁹ Echoing a common sentiment in other hackerspaces, in relation to what happens within and to the hackerspace, “we throw everything out in the open. Too much maybe but we have absolutely no secrets.... Everything is out in the open and we try to spread that, and people automatically accept that”.²⁷⁰ The proclivity for openness and inclusiveness is evident as well at hacker camps where people strive to have a welcoming and festive atmosphere. At camps, save for the police and other public authorities, “[i]t is not acceptable to make others feel unwelcome because they are” different, and “[d]iscrimination, sexism, harassment and dismissive, demeaning and/or offending language are unacceptable”.²⁷¹

For most hackers, being open means embracing, developing and using technologies that are free and open source. At hacker camps, having a black ThinkPad running Linux was de rigueur. FOSS

²⁶⁴ Interview with Hactivist B.

²⁶⁵ Interview with Maker L.

²⁶⁶ Interview with Maker D.

²⁶⁷ Interview with Maker F.

²⁶⁸ Interview with Maker E.

²⁶⁹ Interview with Maker E.

²⁷⁰ Interview with Maker E.

²⁷¹ OHM2013, “Guidelines”.

is definitely one of the principal embodiments of the value of openness. Most of the technologies that makers and hacktivists create and use are released under a FOSS license or are in the public domain.²⁷² Software is often made available on open repositories like GitHub. As Maker A relates, “A lot of stuff is open source. A lot of people who do open source are really open about it”.²⁷³ Maker L explains the appeal of free and open source: “If a project I’m working with is not a closed source project, that’s an open source project or a free software project, people who want to participate are able to participate so it’s not a closed group”.²⁷⁴ The fondness for technologies that are free and open is the reason why the decision of MakerBot to abandon openness and become a closed and proprietary company was exceptionally upsetting for makers. “Yeah, they went from a very open company to a very, very closed company”, states Maker K.²⁷⁵ According to Maker C, “There is always a tension especially because of MakerBot. They came out saying we’re open hardware, change the world, and they ended up selling out to a company and being closed source”. There is a general feeling of disappointment and even betrayal among makers. Maker I explains, “You don’t just say you’re open source, but you actually have to do it. If you don’t, a lot of people will really start disliking you”.²⁷⁶

Openness also makes a lot of sense from a technical and practical perspective. There is a common belief among hackers that free and open is not merely necessary but also inevitable. According to Maker J, “It just doesn’t work to say that you can keep things a secret. Using technology, that’s not going to work”.²⁷⁷ For many hackers, openness is the most sensible approach to technology. As Hactivist D puts it, “Having technology being more open, allowing people to hack it and make it more fit in their lifestyle or their personality is a much more

²⁷² See OHM2013, “FAQ”.

²⁷³ Interview with Maker A.

²⁷⁴ Interview with Maker L.

²⁷⁵ Interview with Maker K.

²⁷⁶ Interview with Maker I.

²⁷⁷ Interview with Maker J.

democratic and more natural approach to technology”.²⁷⁸ The epitome of this approach is the FOSS development model that many hackers subscribe to (see Section 2.2.4).

Openness directly relates to and supports another important hacker value – freedom of access. According to Maker H, “the hacker ethos is about making technology accessible to all people from all walks of life”.²⁷⁹ Similarly, for Hactivist B, hacking represents “an opening to get a more free relationship to technology” and “freedom of access was one of the core values of [the hackerspace] from the beginning”.²⁸⁰ Emphasizing the social dimensions of hacking, Maker D narrates how “I like the project because it gives all citizens access to participating with IT for the society”.²⁸¹ Developing and using open source technologies and projects is integral in ensuring and promoting freedom of access. Maker D explains makers’ experiences with and affection for open source software and hardware, “Everything is available and they don’t feel limited. They feel that they can do everything they want”.²⁸² Maker D further explains, “Open source is very mature. So people can download everything they want and they use it for their own hobby. For software they are not being limited.... For electronics, they can do everything they can because also open source hardware is always available”.²⁸³

3.4.6.2 Transparency

Closely related to openness and freedom of access is the value of transparency. While these values are interconnected and overlap, transparency relates more to the actual state of technical and non-technical systems and structures. So, while openness and freedom of access generally pertain to the rights and capabilities in relation

²⁷⁸ Interview with Hactivist D.

²⁷⁹ Interview with Maker H.

²⁸⁰ Interview with Hactivist B.

²⁸¹ Interview with Maker D.

²⁸² Interview with Maker D.

²⁸³ Interview with Maker D.

to technology, transparency concerns the character or condition of the technology or system itself. Based on my interviews, the goal of transparency is strongest among makers and ethical hackers possibly because of their need to learn the inner workings of technical systems. Maker I explains the rationale for transparency in hacker projects: “usually all of their designs and code and everything is already on Github so you know what you’re getting into”.²⁸⁴ Hactivist C sums up the ideal of transparency whether for technologies or governments: “maximum transparency, minimum overhead and maximum flow”.²⁸⁵

In the same way makers and hacktivists insist on openness and freedom of access in their technologies and communities, they also expect and desire greater transparency from government and social institutions. As Maker L explains, “openness, open data, etc. is very important” but “transparency is also specially for government” very necessary.²⁸⁶ Many makers and hacktivists perceive the government as a monolithic black box and there is palpable animosity and distrust particularly after the Snowden revelations. Some hackers believe that secrecy breeds wrongdoing. They point to the incongruence and even hypocrisy of the situation: “the government wants to know much more about you, but wants to give out less information about itself”.²⁸⁷ While the Dutch government has formally tried to reach out and engage with the hacker community, many hackers share Hactivist F’s feeling that “it cannot be a true reaching out because there’s no transparency. There’s no true transparency. We don’t really know what they’re doing”.²⁸⁸ Hactivists F continues, “The level of knowledge exchange will always be asymmetrical. So they think that there’s very little to win for our communities to engage in that way”.²⁸⁹ Maker L agrees, “They do all those kinds of things [like mass surveillance] but want the

²⁸⁴ Interview with Maker I.

²⁸⁵ Interview with Hactivist C.

²⁸⁶ Interview with Maker L.

²⁸⁷ Interview with Maker L.

²⁸⁸ Interview with Hactivist F.

²⁸⁹ Interview with Hactivist F.

things they do to be kept secret”.²⁹⁰

Hackers and people associated with the hacker community have used freedom of information laws as part of their hacking campaigns and projects. Availing of freedom of information requests, they seek to gain access to critical information and data about and from public authorities. According to one hacker, “If you look at it, it’s a very short law but the implications are very big”.²⁹¹ A hacker points out, “using freedom of information, I can use it against the government to reveal things”.²⁹² For a number of hackers, freedom of information requests can be used to provide more transparency in government and greater freedom of access to public sector information. A few members of the hacker community view freedom of access as close to an absolute right: “Go to the military and police and say we’re paying [for] your system. Open your data and see what you have. They will have to say, ‘No, no, no’. You keep asking ‘Why, why, why?’ And in the end, they’ll say state interest, and you go, which state, what’s left of that state?”²⁹³ However, many hackers have a less radical outlook and they see the benefits of following the necessary procedures since “it’s better to engage in a legal/policy way with those types of institutions through... freedom of information requests”.²⁹⁴

Hackers find out about freedom of information laws either by actually “submitting FOIA requests, attending FOIA events, and sharing FOIA-related news on social media”.²⁹⁵ They also learn from journalists and people “with semi-legal background or at least with experience with freedom of information [laws]”.²⁹⁶ “Most of those guys became street-wise for sending the wrong [requests]. [They now know]

²⁹⁰ Interview with Maker L.

²⁹¹ Interview.

²⁹² Interview.

²⁹³ Interview.

²⁹⁴ Interview.

²⁹⁵ Interview.

²⁹⁶ Interview.

²⁹⁷ Interview.

how you should ask the question that [the government] cannot say no [to]”, explains a hacker.²⁹⁷ Hackers may use a freedom of information procedure “to force [government officials] to state what they stated on the phone on paper”.²⁹⁸

However, resorting to freedom of information laws is neither straightforward nor without difficulties. It is worth noting that freedom of information requests were made in the voting computers campaign but “attempts to retrieve the source code of the machines via the Freedom of Information Act failed, because the source code is intellectual property of the producer” (see Section 5.2.2.2).²⁹⁹ Similar requests were made in relation to the OV-chipcard hacks but they ultimately proved unproductive (see Section 5.2.2.4). A hacker explains the problems they face:

We have freedom of information. We have official rules, but all the time governments, municipalities everywhere find it an annoyance and try to blockade the openness of [the] information as much as possible. So people have to go to court. It takes a lot of time. Yeah, I find that it must be better.³⁰⁰

“They like to fight freedom of information requests”, recounts a hacker, “Postpone them as much as they can... yeah you see that a lot”.³⁰¹ Furthermore, even if public authorities do respond, the information they provide is often not very useful because “all the interesting questions were not answered, because of... it’s important to the country not to reveal it... national security”.³⁰²

Makers and hacktivists would really like to see greater transparency in government. For Maker L, transparency is critical for democracy and fairness: “If a government wants to know a lot about me, I sure want to know everything from my government”.³⁰³ While there are

²⁹⁸ Interview.

²⁹⁹ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 11.

³⁰⁰ Interview.

³⁰¹ Interview.

³⁰² Interview.

³⁰³ Interview with Maker L.

some hackers who subscribe to a radical form of government transparency, there are those like Maker J who “don’t really subscribe to the whole freedom of information philosophy. I think there is some information that doesn’t have to be free necessarily”.³⁰⁴ However, Maker J clarifies, “but I do believe that for the most important things, we need to be transparent about how they work, how they operate”.³⁰⁵ Ethical Hacker B agrees that even just “a bit of transparency would be nice, and even that can be achieved with technology. But you know in that sense there’s a lot possible but I don’t know if everyone wants it”.³⁰⁶ It is interesting to note that the Dutch national and local governments have supported a number of open data initiatives and projects but the greatest hurdle to achieving a more transparent government is political or cultural rather than technical.³⁰⁷ Based on personal experience, Maker B explains that the primary impediments to greater government transparency and open data are “cultural because technical[ly] it can be solved”.³⁰⁸

3.4.6.3 Security

The hackers I met are very security conscious. They make it a point to make their computers and network connections safe and secure by, among others things, modifying and hardening their laptops, running more security-focused operating systems or software, using strong passwords, employing encryption, locking their computers when they are away, preferring to connect to the internet via wired rather than wireless connections, and accessing the Web using virtual private networks. Hacker camps are considered technology and security conferences and many of the presentations and hands-on workshops are about information security.³⁰⁹

³⁰⁴ Interview with Maker J.

³⁰⁵ Interview with Maker J.

³⁰⁶ Interview with Ethical Hacker B.

³⁰⁷ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 9; see Anneke Zuiderwijk and others, “Socio-technical Impediments of Open Data”.

³⁰⁸ Interview with Maker B.

³⁰⁹ See OHM2013, “Call for Participation”.

Hackers I interviewed wholeheartedly agree that security is extremely important because of its intrinsic connection with other hacker values. Hactivist D explains, “with individual autonomy and liberty, you only can achieve that if like privacy, security and anonymity are already there”.³¹⁰ For Ethical Hacker B, “There are these kind of terms which are often placed closed to other terms like privacy, anonymity, but now I guess they are covered by the term security”.³¹¹ Based on my interviews, ethical hackers and hactivists especially place great store on security because, for the former, they primarily engage in testing and securing systems and, for the latter, the security of their persons and computers is a main concern when they undertake socio-political campaigns. Ethical hackers in particular understand that in order to properly secure a technology or system, they first have to explore and learn how it works and this requires breaking or knowing how to break it. According to Ethical Hacker A, “The first step in attacking a system is knowing how it works, being able to work with it”.³¹² Securing systems and technologies is all the more difficult because, as Maker G says, “Systems are really complex. And if you want to defend, you have to find all the bugs. And if you want to attack, you have to find one”.³¹³

While not all hackers are security professionals, they are all concerned about security and they see the importance of people using secure and robust technologies and fixing those that have security vulnerabilities. Maker H relates, “Hacking doesn’t necessarily have to do with IT security, but there is a growing influence on at least the IT security aspect”.³¹⁴ Despite or possibly because of their technical adeptness, most hackers I met view technology with a critical eye and have a healthy distrust of it. Ethical Hacker A explains the problem with security and technology:

³¹⁰ Interview with Hactivist D.

³¹¹ Interview with Ethical Hacker B.

³¹² Interview with Ethical Hacker A.

³¹³ Interview with Maker G.

³¹⁴ Interview with Maker H.

So that's also something that makes it really interesting for me is that we don't, in my opinion, should trust on technology only. Or if you're trusting on technology, in my opinion, you should open the technology and allow everyone to look at it and have a fair discussion about possible weaknesses in it.... So I think, hacking or security testing is a very interesting tool to prove that things are not OK.³¹⁵

This skepticism is appropriate given that, as Maker J notes, "I was sort of surprised and appalled by the state of security in infrastructures that we have currently".³¹⁶

Security is therefore seen as both a technical and a social imperative. Hactivist E unequivocally states, "If vulnerabilities exist, they must be found and fixed".³¹⁷ For Maker B, the role of the hacker community is to act as "a kind of public watchdog for IT quality".³¹⁸ "As hackers, it's important for us to let policymakers, let lawmakers, the Parliament etc., know what those risks are", explains Maker L.³¹⁹ Maker J concurs, "I also feel that my knowledge helps me to improve the situation for security".³²⁰ While hacking for the purposes of security testing has yet to gain widespread public acceptance, hackers unanimously agree that "bringing vulnerabilities to light is positive and constructive".³²¹ Hackers believe that they do not actually break systems but merely identify weaknesses in them since the systems were already broken in the first place because of existing vulnerabilities. As Ethical Hacker B argues, "It's not that someone here actually makes something broken, but just identifies a weakness".³²²

³¹⁵ Interview with Ethical Hacker A.

³¹⁶ Interview with Maker J.

³¹⁷ Interview with Hactivist E.

³¹⁸ Interview with Maker B.

³¹⁹ Interview with Maker L.

³²⁰ Interview with Maker J.

³²¹ Interview with Maker H.

³²² Interview with Ethical Hacker B.

3.4.6.4 Privacy

Last but far from being least, the value of privacy remains crucial for makers and hacktivists. As privacy is a complex subject and conceptually difficult to qualify and quantify, there is no unanimity among hacker as to what privacy definitely means. For some, privacy is about one's private life being free from the scrutiny or interference of others especially the government and commercial companies. Maker L feels that his privacy is infringed by extensive government surveillance: "You don't, sometimes you don't have the feeling, am I free to move around this country anymore without being tracked by the government where I am at any point?"³²³ For other hackers, privacy is about independence or autonomy over one's personal life or private information. As Hactivist D explains, "I think it's also a very one-dimensional idea of what privacy is. Privacy is not about keeping your data to yourself. Privacy for me is much more about having control and agency in which aspects... are known about you".³²⁴ Hactivist E agrees, "privacy is a problem of autonomy".³²⁵

What makes the matter of privacy all the more complicated is that it is inherently interconnected with other values. "You cannot have freedom of expression without privacy", claims Hactivist F. According to Hactivist E, "We're in a continuous split as well when it comes, for instance, [to] privacy and security".³²⁶ But hackers like Maker L argue that "people put it that privacy and security, is you have to pick one over the other, and I don't agree with that".³²⁷ Maker L believes, "You can be open but have your privacy".³²⁸ Hactivist D supports this position by explaining, "There are many different moments in my life where I decided to give up some of my privacy to share like being

³²³ Interview with Maker L.

³²⁴ Interview with Hactivist D.

³²⁵ Interview with Hactivist E.

³²⁶ Interview with Hactivist B.

³²⁷ Interview with Maker J.

³²⁸ Interview with Maker L.

onstage talking to a lot of people”.³²⁹ But Hactivist D clarifies, “But it’s much more about being in charge. That I am the one deciding that these 400 people are going to hear it and nobody else but them”.³³⁰

While hackers may not completely see eye-to-eye on the exact meaning of privacy and how best to achieve it, they are in full agreement that it is an important value that must be preserved and protected. At hacker camps, taking photographs or videos of people is strictly frowned upon since “many participants are not keen on being in pictures, movies or audio recordings without their consent”.³³¹ Hackers’ concerns about privacy became extremely heightened in the aftermath of the Snowden revelations. Maker D recounts, “Privacy became the highest priority... when Snowden got out and warned us all”.³³² The Snowden leaks confirmed what a number of hackers had suspected all along. Whether through the actions of governments and commercial companies or the technologies and systems they use, “I see a very big threat to privacy in the way that society is developing currently”, says Maker J.³³³ For Maker L, “I see in this country but all over the world losing more and more privacy”.³³⁴ There is a high degree of distrust and animosity among hackers toward governments, companies and even their own technologies. Hactivist D relates, “I don’t trust my own machine. You know I have a laptop at home, which I generally don’t trust. I also have my telephone. I have a sticker over my camera”.³³⁵ Hactivist D continues, “People think privacy is important but they have mechanical machines around them that they don’t understand. They feel the machines are threatening their privacy”.³³⁶

Post-Snowden, there has been a discernible increase in the

³²⁹ Interview with Hactivist D.

³³⁰ Interview with Hactivist D.

³³¹ OHM2013, “FAQ”.

³³² Interview with Maker D.

³³³ Interview with Maker J.

³³⁴ Interview with Maker L.

³³⁵ Interview with Hactivist D.

³³⁶ Interview with Hactivist D.

number of hacker projects that directly deal with the matter of privacy and security. According to Maker G, in the Dutch hacker scene, “yeah I guess there’s some extra enthusiasm to getting more projects to defend against this”.³³⁷ Projects that make privacy and security tools more accessible and usable are on the rise and hackers like Maker J agree that, “I think that’s a very good development”.³³⁸ For example, members of the hacker community have organized public workshops that are “basically about inviting people over for a 3-hour workshop with their laptops. And then we have like a menu of different tools you can install and we try to empower people to feel more in control of their machines”.³³⁹ While there is still heightened tension and anxiety and sometimes even paranoia among the hackers, on the whole, they have chosen a very self-reliant and do-it-yourself attitude and response to the problem of government surveillance and other threats to their privacy. Ethical Hacker B explains the constructive and pragmatic approach that many hackers have adopted concerning privacy and technology, “In general, if you really think something is violating privacy then I’d rather think of trying to expose it or fix it even, than to just dig myself into some hole saying I don’t want to use it”.³⁴⁰ Maker L concurs, “It’s hard to keep your privacy. Sometimes you can’t, so then you make the best choice you can. But if possible I make the choice to keep my privacy”.³⁴¹

3.5 Normatively full and value-laden

With respect to their norms and values, makers and hacktivists share many things in common. The values of creativity and innovation, curiosity, and individual autonomy and liberty rank highest for both of them. Makers and hacktivists also place great importance on having

³³⁷ Interview with Maker G.

³³⁸ Interview with Maker J.

³³⁹ Interview.

³⁴⁰ Interview with Ethical Hacker B.

³⁴¹ Interview with Maker L.

free and open access to and use of information and technology. But there are differences between them as well. While they both highly prize community development and social development, makers place greater emphasis on the former whereas hacktivists have the end goal of social development when undertaking their hacking projects and activities. Their stronger concern for community development may be explained by the fact that makers regularly interact and spend more time with other makers in their hackerspaces. In contrast, hacktivists have fewer opportunities to socialize with one another and their interactions are often focused more on furthering their campaigns and causes. Makers also place added emphasis on openness and transparency because they need to have full access to technologies and systems in order to use them in new and interesting ways. On their part, hacktivists consider privacy and security to be of utmost importance. Compared to makers, hacktivists spend considerable attention and resources making sure that their and other people's technologies, systems and communications are private and secure due in no small part to the more serious and heavier nature of their activities.

Based on my empirical findings and in contrast to how hackers are generally depicted in popular and mass media, the makers and hacktivists I met are not malicious, antisocial outlaws who are out to steal information and damage computers. In light of their norms and values, makers and hacktivists prize and strive to produce technical creativity and innovation for their own and other people's benefit. While their activities may be disruptive, they are not motivated by malice but are simply curious about learning how something works. Even though they cherish their individual autonomy and liberty, makers and hacktivists are very much socially conscious and community focused in their orientation and actions. Furthermore, they endeavor and aspire to achieve personal and social goals such as greater openness and freedom of access to technology, more transparency in government,

better security of information systems, and stronger privacy protection.

It bears stressing though that hacker norms and values are never stable or at rest, and neither do they exist peacefully in separate domains. They are in fact inherently and constantly interacting with each other. For instance, makers and hacktivists espouse openness and freedom of access to information and technology, but they are equally concerned with ensuring the privacy and security of computer systems and data. Based on my observations, makers and hacktivists are able to partly resolve this apparent incongruity by creating and using technologies and undertaking activities that are specific to some but not all of their values. For example, in relation to open source 3D printers, privacy and security are not major concerns and the primary focus of this technology is openness, creativity and innovation, and freedom of access. Privacy and security though are essential when hacktivists produce or use anonymization tools, encryption software, and other security- and privacy-enhancing technologies. By compartmentalizing or tying their norms and values to the specific purposes and functions of different technologies, they are able to avoid some of these issues and contradictions. However, hackers' modular approach to technology vis-à-vis their norms and values cannot resolve all the conflicts that arise. For instance, while penetration testing software and tools are designed for testing and improving the security of computer systems, they have also been used to compromise computers and breach the privacy of users. This means that makers and hacktivists cannot depend solely on technical design decisions to address these inconsistencies. Consider the values of individual autonomy and liberty and social development. While the hackers I spoke to seem to be able to strike a balance whereby they use their individual freedoms to achieve communal and social goals, there is no true equilibrium and things are never completely settled. There is a constant push and pull between varying and competing priorities and interpretations of these and

other values. There are some hackers who believe in complete transparency and would not hesitate in disclosing any information that they discover, even it includes the personal data of ordinary users. There are a few makers who would pursue curiosity and creativity and innovation above all despite the potential risks to themselves and others. But what aids makers and hacktivists better deal with these conflicts, is that they do not hack in isolation, they socialize with other hackers and they imagine themselves as belonging to the hacker community and the wider society. Being socially consciousness and active helps them go beyond their personal preferences and reconcile the tensions between their individual freedoms and their social responsibility.

Much attention, space and time have been devoted in this and the preceding chapter to describing and explicating the characteristics and nuances of hacker culture, norms and values, especially with regard to makers and hacktivists. Taking such a deep and prolonged dive into makers' and hacktivists' social worlds and their ways of meaning-making is crucial because it is a necessary and foundational step to more fully understanding the explicit and implicit reasons, intentions and motivations for their actions, beliefs and technological creations. As this chapter has shown, hackers are not value-free individuals and groups, and neither do they exist in a normative vacuum. Far from being "lawless" people or existing in a state of anomie, makers and hacktivists possess and perform multiple norms and values, and the social fields and spaces they inhabit and the technologies they produce are "normatively full"³⁴² and thickly value-laden.

³⁴² John Griffiths, "What is Legal Pluralism?" 34.

The ways makers and hacktivists interpret and defend their varied norms and values (especially in times of crisis and change) can reveal a lot about why they act the way they do within their communities, and, equally important, how they react to external influences, threats and interferences particularly those arising from law and public authorities. The essentiality of studying the interactions and conflicts between norms and values becomes indisputable when one recognizes that laws themselves express and enact expectations, evaluations, and prescriptions of the appropriate and the desirable. There is indeed much benefit to be derived from similarly applying a normative and values-based approach to the analysis of the relevant laws on hacking, which is dealt with in the following chapter.

CHAPTER FOUR

Laws on hacking

This chapter analyzes the technology laws and policies that are most relevant to hacking. There are a number of laws that specifically apply to makers and hacktivists. These laws on hacking involve matters such as computer crime, intellectual property, contract, anti-circumvention, consumer protection, human rights (e.g., freedom of expression and privacy), data protection, trade secrets, and state secrets. While these areas of law possess their own distinct concepts and operate according to discrete legal regimes, what ties them all together and connects them to hacking is that, like hacking, they essentially deal with or concern access to and use of information and technology. As the foregoing chapters have shown, freedom and openness of information, knowledge and technology is a central purpose and *conditio sine qua non* of hacking.¹ In this way, the question of whether these hacking-related laws and policies tend to restrict or support access to and use of information and technology primarily frames the discussion and analysis in this chapter. It should be noted though that while all of the above laws are pertinent to hacking, the focus of this chapter is mainly on those areas of law that were most talked about and deemed most relevant by the makers and hacktivists that I spoke to, namely: computer crime, intellectual property, contract, and anti-circumvention. While this chapter does not specifically delve into human rights law, throughout this book, the discussion and analysis of hacker norms and values such as privacy, individual autonomy and liberty, freedom of expression and freedom of information are informed by human

¹ See David Wall, *Cybercrime* 55.

rights considerations.

4.1 A normative and axiological approach

Laws are unquestionably normative and value-laden. They manifestly enact and express prescriptive rules and normative statements about the acceptable and the desirable.² In this sense, doctrinal legal research is fundamentally concerned with normative matters and issues. But, while traditional legal research basically involves the identification, interpretation or application of legal principles and rules in relation to specific facts and cases to produce legally authoritative judgments or opinions,³ this chapter advances a methodological approach that includes but also goes beyond conventional doctrinal analysis. In examining the laws on hacking, considerable effort and attention are devoted to identifying and elucidating the explicit and implicit norms and values embodied in these laws. Such a normative and axiological (i.e., values-centered) approach is neither new nor alien to the fields of socio-legal studies and STS.⁴ It bears noting though that the kind of axiology utilized in this chapter is less concerned with purely philosophical or abstract ruminations about ethics, but strives to identify, ground and examine norms - values in actual practices and everyday experiences through the use of empirical methods and data. Examining and taking account of the values of the research subjects, the researcher and their social worlds is crucial to social science research.⁵ In STS, two of the key premises and preoccupations of the discipline are the recognition that technologies have values and that values are central to the production of science and technology.⁶ Besides studying the intrinsic and extrinsic values of technology, some

² See Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation 5-6* (on the facilitative and expressive functions of law); see also Cass Sunstein, "On the Expressive Function of Law".

³ See William Twining and David Miers, *How to Do Things With Rules 131*; see Ian Curry-Summer and others, *Research Skills: Instruction for Lawyer 3-4*.

⁴ Maggie Walter, *Social Research Methods 13*; see Samuel Hart, "Axiology - Theory of Values".

⁵ Maggie Walter, *Social Research Methods 13*.

⁶ See Cory Knobel and Geoffrey Bowker, "Values in Design" 2; Batya Friedman and Helen Nissenbaum, "Bias in Computer Systems" 335.

STS scholars have undertaken “public value mapping” in order to evaluate the social impact and outcomes of science and technology policies.⁷ A vital part of public value mapping is searching for, identifying and examining the relations between values in a wide range of legal and documentary sources such as laws and legislative histories, policies and policy statements, government strategic plans and documents, pertinent academic literature, and public discourse and debates on the subject.⁸

The normative and axiological approach applied in this chapter therefore combines doctrinal legal research with qualitative content analysis of the relevant laws, policies, regulations, rulings and other legal statements and actions, with a specific view to identifying the normative statements and rules contained in these laws and legal actions and their explicit and implicit value positions and commitments, and, consequently, how they relate to or conflict with the norms and values of hackers. Despite the seeming primacy given to documentary sources, the corresponding behaviors and actions of public authorities and state actors are also very much considered and taken into account in order to more fully analyze and contextualize the norms and values found in these laws and policies.

It should be noted that the succeeding analysis is particularly geared towards and framed according to the norms, values and worldviews of hackers vis-à-vis the law. The laws on hacking are therefore principally examined and assessed based on the specific subject positions and unique perspectives of makers and hacktivists. Being able to see and evaluate the law “through their eyes” is an invaluable aspect of the socio-techno-legal approach espoused by this book because it reveals the reasons why makers and hacktivists view and respond to

⁷ See Barry Bozeman and Daniel Sarewitz, “Public Value Mapping and Science Policy Evaluation”; see Erik Fisher and others, “The public value of nanotechnology”.

⁸ Barry Bozeman and Daniel Sarewitz, “Public Value Mapping and Science Policy Evaluation” 6, 15, 18 and 19; Erik Fisher and others, “The public value of nanotechnology” 31.

laws in the way they do.

Of the laws that are material to hacking, computer crime laws and intellectual property laws are without doubt the most significant and consequential to makers and hacktivists. This is not surprising given that computer crime legislations specifically target activities concerning illegal or unauthorized access and use of computer systems and data, and intellectual property laws are chiefly concerned with the exclusive rights of control over access to and use of information, content and know-how.⁹ Much of the exploration and discussion below center on these two fields, but other areas of law are tackled and remain relevant in the analysis.

4.2 Computer crime laws

4.2.1 BRIEF HISTORY AND DEVELOPMENT

As touched on in the underground hackers section in Section 2.2.3, a number of factors and conditions led to the outlawing and criminalization of hacking.¹⁰ Beginning in the 1980s, governments around the world enacted computer crime laws and intensified prosecutions and enforcement activities against hacking-related activities.¹¹ In the United States, for example, “[t]he first federal computer-crime legislation was proposed in 1979” but it was not formally adopted until 1984.¹² This federal law was subsequently revised to “set up a more comprehensive legal framework for the prosecution of computer crimes”,¹³ and became the US Computer Fraud and Abuse Act (US CFAA).¹⁴ The US CFAA like other computer crime laws concerns

⁹ See Recommendation No. R (89) 9 on computer-related crime 54; see Lawrence Lessig, Code: version 2.0 171.

¹⁰ See Jay BloomBecker, “Computer Crime Update” 628 and 637.

¹¹ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 581-582; Ian Lloyd, Information Technology Law 215; Tim Jordan, Hacking 39.

¹² Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 582 (citations omitted); see also Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1615.

¹³ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 582 (citations omitted); see also Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1615; see also Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) Computer Law 242.

the prohibition of “a variety of acts involving the use of computers”¹⁵ and “the prosecution of certain crimes accomplished by means of a computer”. It bears noting that the first computer crime laws in the United States were enacted by state legislators in Florida and Arizona as early as 1978,¹⁶ but, until 1984, less than 200 cases were prosecuted and fewer still went to trial under these and other subsequent state computer crime laws.¹⁷ Most of these cases involved insiders (i.e., disgruntled employees or disloyal agents) who exceeded their authority instead of outside hackers who had no authority at all to access the relevant computers.¹⁸ A number of European countries similarly passed their own computer crime statutes in the 1980s and early 1990s.¹⁹ It is notable that Germany, the Netherlands, Italy and Finland adopted computer crime laws notwithstanding or possibly because of the existence of prominent and distinctly recognizable hacker tradition and cultures within their respective jurisdictions.²⁰ As with the US CFAA, European computer crime laws prohibit and penalize various acts and conduct, most specifically “unauthorized access”, “trespass” and “causing damage” to computers and data.²¹

With the greater availability and use of computers and their interconnection with wider and ultimately global information and communications networks from the 1980s onwards, computer crime has become a growing national, regional and international concern and many state actors have sought to address or find solutions to it.²²

¹⁴ Richard Hollinger, “Computer Crime” 78; Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 584; Cyrus Chung, “The Computer Fraud and Abuse Act” 236; Reid Skibell, “Cybercrimes & Misdemeanors” 912.

¹⁵ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 584-585

¹⁶ Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 101; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1615.

¹⁷ Jay BloomBecker, “Computer Crime Update” 645; Richard Hollinger, “Computer Crime” 78; Cyrus Chung, “The Computer Fraud and Abuse Act” 239; Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) Computer Law 245; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1630; Reid Skibell, “Cybercrimes & Misdemeanors” 939.

¹⁸ Richard Hollinger, “Computer Crime” 78; Cyrus Chung, “The Computer Fraud and Abuse Act” 239; Jay BloomBecker, “Computer Crime Update” 645; Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) Computer Law 245; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1630; Reid Skibell, “Cybercrimes & Misdemeanors” 939.

¹⁹ Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) Computer Law 242.

²⁰ Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) Computer Law 242.

²¹ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 585; Cyrus Chung, “The Computer Fraud and Abuse Act” 237; Charles Doyle “Cybercrime”; Ian Lloyd, Information Technology Law 209; Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) Computer Law 262.

For instance, the Organisation for Economic Co-operation and Development (OECD) has published reports, guidelines, recommendations and implementation plans on computer-related crime and information security since the mid-1980s.²³ The OECD's proposed policies on computer crime were addressed to international and regional bodies, state agencies, private entities and even individual computer users.²⁴ However, the establishment of a formal and harmonized international legal regime on computer crime would only take place after the start of the millennium through the adoption of the Council of Europe's Convention on Cybercrime (the Convention on Cybercrime).²⁵ The Convention was released for ratification in 2001 and was the outcome of years of discussions and consultations among governments and other interested parties.²⁶ The Convention entered into force in 2004 and, at the time of writing, has been ratified or acceded to by 48 states and counting, including quite a number of countries outside of Europe like the United States, Australia and Japan.²⁷ All EU Member States have signed the Convention and most have formally ratified it.²⁸

The Convention on Cybercrime is widely "regarded as the most complete international standard to date, since it provides a comprehensive and coherent framework embracing the various aspects relating to cybercrime".²⁹ As "the leading international instrument" on computer crime, many of the Convention's principles and provisions have been replicated or translated into regional and national laws.³⁰

²² Ian Lloyd and Moira Simpson "Computer Crime" in Chris Reed (ed) *Computer Law* 242.

²³ Ian Lloyd, *Information Technology Law* 217-218; Ian Lloyd and Moira Simpson "Computer Crime" in Chris Reed (ed) *Computer Law* 242.

²⁴ Ian Lloyd, *Information Technology Law* 217-218.

²⁵ Ian Lloyd, *Information Technology Law* 216-217; Convention on Cybercrime <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>> accessed 26 July 2013.

²⁶ Lorenzo Picotti and Ivan Salvadori, "National legislation implementing the Convention on Cybercrime" 4; Ian Lloyd, *Information Technology Law* 216-217; Convention on Cybercrime <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>> accessed 26 July 2013.

²⁷ Convention on Cybercrime <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>> accessed 29 January 2016; Lorenzo Picotti and Ivan Salvadori, "National legislation implementing the Convention on Cybercrime" 4.

²⁸ Convention on Cybercrime <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>> accessed 11 December 2014; see Commission, "Proposal for a Directive on attacks against information systems" COM(2010) 517, 2.

²⁹ Commission, "Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA" COM(2010) 517, 2; see also Lorenzo Picotti and Ivan Salvadori, "National legislation implementing the Convention on Cybercrime" 4.

The European Union for its part adopted Council Framework Decision 2005/222/JHA on attacks against information systems (the Framework Decision) in 2005 and, like the Convention on Cybercrime, it “requires that Member States criminalise the acts of attempting or obtaining illegal access to or perpetrating illegal interference with, information systems, together with acts intended to instigate, aid, or abet the practice”.³¹ In 2013, the Framework Decision was replaced by Directive 2013/40/EU on attacks against information systems (the Cybercrime Directive).³² The aim of the Directive is to build on the Framework Decision and the Convention of Cybercrime and “amend and expand” the legal rules and processes in light of current practices and technologies used in cybercrime particularly the creation and use of “botnets” to carry out large-scale attacks.³³ The primary objective of the Directive is “to approximate the criminal laws of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions”.³⁴ It seeks to accomplish this by having a “common approach” across the European Union with regard “to the constituent elements of criminal offences by introducing common offences”.³⁵ The Convention on Cybercrime and the Directive criminalize “offences against the confidentiality, integrity and availability of computer data and systems”.³⁶ These acts fall under the general category of “computer security crimes”.³⁷

³⁰ Ian Lloyd, *Information Technology Law* 221; see also Council Directive 2013/40/EU on attacks against information systems, recital 15.

³¹ Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [2005] OJ L069; Ian Lloyd, *Information Technology Law* 218-219.

³² Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

³³ Council Directive 2013/40/EU on attacks against information systems, recitals 5, 15 and 34; see Commission, “Proposal for a Directive on attacks against information systems” COM(2010) 517, 3.

³⁴ Council Directive 2013/40/EU on attacks against information systems, recital 1.

³⁵ Council Directive 2013/40/EU on attacks against information systems, recital 8.

³⁶ Convention on Cybercrime, Title I; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 13.

³⁷ See David Wall, *Cybercrime* 10, 49 and 53 (who prefers to use the term “computer integrity crimes”).

4.2.2 COMPUTER CRIME AND HACKING

Criminalization may be deemed to be the most forceful response of the law and authorities to hacking activities and technologies.³⁸ Computer crime laws prohibit certain forms of hacking by declaring them to be illegal and imposing criminal liability and penalties like imprisonment and fines on those who engage in such acts or conduct. Equating hacking to criminality and deviance has profound consequences for makers and hacktivists.³⁹ By broadly outlawing and prosecuting hacking-related activities, computer crime laws tend to restrict and hinder the capability of makers, hacktivists and other types of hackers to creatively and constructively access and use information and technology.

In contrast to the more complex and dense meaning of hacking propounded in this book, under the Convention on Cybercrime and related or analogous regional and national computer crime laws and policies, hacking is used as a generic term to describe “the basic offence of dangerous threats to and attacks against the security (i.e., the confidentiality, integrity and availability) of computer systems and data”.⁴⁰ While hacking per se is not formally and specifically defined and criminalized under the Convention or the Cybercrime Directive, the term is repeatedly used by public authorities and the media as a shorthand for activities that impair the security and integrity of computers.⁴¹ Computer crime laws are sometimes called “anti-hacking statutes”.⁴² It may not have been the law’s intention, but hacking has nonetheless been associated and lumped together with computer crime.⁴³ As a result, many projects and activities of makers and hack-

³⁸ See Reid Skibell, “Cybercrimes & Misdemeanors” 943.

³⁹ Helen Nissenbaum, “Hackers and the contested ontology of cyberspace” 196; Debora Halbert, “Discourses of Danger and the Computer Hacker” 364; Reid Skibell, “The Myth of the Computer Hacker” 349.

⁴⁰ Explanatory Report to the Convention on Cybercrime, paras 35, 44 and 49.

⁴¹ David Wall, Cybercrime 10, 49 and 53; Explanatory Report to the Convention on Cybercrime, paras 44 and 71; see Juerd Waalboer and others, “Open letter to public prosecutor: Hacking”; see Pedro Freitas and Nuno Goncalves, “Illegal access to information systems and the Directive 2013/40/EU” 55; see Debora Halbert, “Discourses of Danger and the Computer Hacker”.

⁴² See Marcia Hofmann and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; see Michael Dizon, “Rules of a networked society” 92.

⁴³ David Wall, Cybercrime 10, 49 and 53; see also Explanatory Report to the Convention on Cybercrime, para 44.

tivists end up being viewed as *prima facie* illegal and potentially in violation of the five kinds of computer security crimes: illegal access, illegal interception, data interference, system interference, and misuse of devices.⁴⁴

4.2.3 ILLEGAL ACCESS

4.2.3.1 Access or entry without right

Illegal or unauthorized access is generally considered to be the essence or crux of computer security crime.⁴⁵ Under the Convention on Cybercrime, illegal access is committed by intentionally accessing “the whole or any part of a computer without right”.⁴⁶ In technical terms, access involves entering any part or aspect of a computer or information system including “hardware, components, stored data of the system installed, directories, traffic and content-related data”.⁴⁷ The phrase “without right” may be understood as referring to “conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law”.⁴⁸ The Cybercrime Directive specifically defines “without right” as that “which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law”.⁴⁹ It must be “understood in a broad sense and including persons who are not entitled to act as they did either in their own right or by authority of those who had a right”.⁵⁰ Therefore, both outsiders (who have no authority to access a

⁴⁴ Explanatory Report to the Convention on Cybercrime, para 43; see David Wall, *Cybercrime* 10, 49 and 53.

⁴⁵ See Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 585 and 622; see Cyrus Chung, “The Computer Fraud and Abuse Act” 236; see Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1597, 1615 and 1616; see Ian Lloyd, *Information Technology Law* 222.

⁴⁶ Convention on Cybercrime, art 2.

⁴⁷ Explanatory Report to the Convention on Cybercrime, para 46; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 14.

⁴⁸ Explanatory Report to the Convention on Cybercrime, para 38.

⁴⁹ Council Directive 2013/40/EU on attacks against information systems, art 2 (d); see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 13.

⁵⁰ Recommendation No. R (89) 9 on computer-related crime 46.

computer system) and insiders (who have exceeded their authority) can commit this offense.⁵¹

Under computer crime laws, mere entry, intrusion or access to a computer without right or sans the permission of the owner is already a punishable offense.⁵² In crafting the provision on illegal access in this way, the drafters opted for a broad application of and a restrictive approach to criminalization.⁵³ While it is true that the Convention grants state parties the option to include “additional qualifying circumstances” for the commission of the crime,⁵⁴ such as “infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the special requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system”,⁵⁵ the United States and most European countries chose the default position and did not incorporate any of these qualifications into their national laws.⁵⁶ A handful of countries opted to include either infringing security measures or special or dishonest intent as an element of illegal access.⁵⁷ The Netherlands, which originally required infringing a security measure as a requisite for committing illegal access, removed this condition when the relevant Dutch law was amended in 2006.⁵⁸

In a curious development though, the requirement of infringing of a security measure has been made mandatory under the updated

⁵¹ See Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1630; see Recommendation No. R (89) 9 on computer-related crime 52; see Ken Lindup, “The Cyberpunk Age” 645; see Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 590 (on a US court ruling that an authorized computer user can be held liable for unauthorized access when he enters parts of the system that he has no authority to access); see Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 102.

⁵² Explanatory Report to the Convention on Cybercrime, para 44; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 14 and 17.

⁵³ Explanatory Report to the Convention on Cybercrime, para 40 and 49.

⁵⁴ Convention on Cybercrime, arts 2, 3, 7 and 8; Explanatory Report to the Convention on Cybercrime, para 59.

⁵⁵ Convention on Cybercrime, art 2; Explanatory Report to the Convention on Cybercrime, para 49 and 50.

⁵⁶ Commission, “Report based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information system” COM(2008) 444, 14 July 2008, 4; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 15.

⁵⁷ Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 14.

⁵⁸ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 7.

Cybercrime Directive.⁵⁹ European policy makers have not proffered an explicit reason why this new requirement has been included.⁶⁰ It is worth noting that “infringing security measures” was part of the original wording of the crime of unauthorized access that was proposed by the Select Committee of Experts on Computer-related Crime, which was originally tasked by the Council of Europe’s European Committee on Crime Problems to study the issue of computer-related crime in the mid to late 1980s.⁶¹ Further, European lawmakers appear to impliedly agree with a proposal made by the legal scholar, Orin Kerr, that illegal or unauthorized access should be limited to “access that circumvents restrictions by code”.⁶² Kerr explains the rationale for limiting illegal access to cases where there is an infringement of a security measure:

... the normative challenge of unauthorized access statutes is to mediate the line between openness on the one hand, and privacy and security on the other.⁶³

Construing “without authorization” to include both the circumvention of code-based barriers and breaches of contract simply draws the line in the wrong place. It grants computer network owners too much power to regulate what Internet users do, and how they do it, sacrificing a great deal of freedom for a small (and arguably minimal) gain in privacy and security.⁶⁴

.... my proposal to limit the scope of unauthorized access to the circumvention of code-based restrictions draws a more balanced line between openness and privacy that carves out zones for each. The proposal would allow Internet users to use the Internet, visit websites, and send e-mails without the chilling effect of possible criminal sanctions arising from the breach of Terms of Service, Terms of Use, or other contractual terms. My proposal would not trigger a cyberspace free-for-all: Users would still be regulated both by contract law and traditional criminal laws, just

⁵⁹ Council Directive 2013/40/EU on attacks against information systems, art 3.

⁶⁰ Pedro Freitas and Nuno Goncalves, “Illegal access to information systems and the Directive 2013/40/EU” 59-60.

⁶¹ Recommendation No. R (89) 9 on computer-related crime 51.

⁶² Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1649.

⁶³ Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1650.

⁶⁴ Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1650.

as they would be off-line. However, unauthorized access laws would no longer threaten to transform disagreements with computer owners into criminal violations.⁶⁵

Kerr's position is seemingly confirmed in one of the recitals of the Cybercrime Directive, which states that "contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability".⁶⁶ According to Freitas and Goncalves, the legal and policy implication of the new requirement is that infringing a security measure is "now considered a minimum legal standard that national States can further develop or not" and/or "the minimum rules concerning illegal access that were established by the European Union in Article 2 (1), of the Framework Decision 2005/222/JHA go beyond what is required in the current state of affairs".⁶⁷ The inclusion of infringing a security measure as an additional element of the crime of illegal access is a notable development in computer crime laws in Europe.

4.2.3.2 Objectives and justifications

The Convention on Cybercrime's restrictive approach to computer security crimes can be further explained and justified in relation to the norms and values that the drafters sought to uphold or realize. The express statements and rules about the acceptable and the desirable contained in the Convention, particularly its Preamble, cluster around three main concerns: (1) deterrence, prosecution or correction of inappropriate or undesirable behavior; (2) promotion of innovation and technology use and development; and (3) protection of public safety and order. Of the three, the first is the principal focus of the Convention as evidenced by such declarations as the necessity to: "de-

⁶⁵ Orin Kerr, "Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" 1651.

⁶⁶ Council Directive 2013/40/EU on attacks against information systems, recital 17.

⁶⁷ Pedro Freitas and Nuno Goncalves, "Illegal access to information systems and the Directive 2013/40/EU" 59.

ter action directed against... computer systems, networks and computer data as well as [their] misuse”, “effectively combating such criminal offences, by facilitating their detection, investigation and prosecution”, and “make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence”.⁶⁸

In relation to the value of promoting innovation, the Convention asserts the need “to protect legitimate interests in the use and development of information technologies” and “to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe”.⁶⁹ When they speak about preventing “damage to legitimate interests”, the drafters of the Convention for the most part refer to the individuals and organizations that own, control or commercially develop computer systems and data.⁷⁰ It is worth quoting at length the reasoning behind criminalizing mere access:

The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. “hacking”, “cracking” or “computer trespass” should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computerrelated offences, like computerrelated fraud or forgery.⁷¹

Illegal access is therefore also viewed as a “basic offense” that

⁶⁸ Convention on Cybercrime, Preamble; see also Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 114 and 115; see also Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1656; see also Reid Skibell, “Cybercrimes & Misdemeanors” 934.

⁶⁹ Convention on Cybercrime, Preamble.

⁷⁰ Explanatory Report to the Convention on Cybercrime, para 9.

⁷¹ Explanatory Report to the Convention on Cybercrime, para 44.

can potentially lead to the carrying out of other, more serious cyber attacks or crimes.⁷²

The third value of public safety and order is stated succinctly as “the protection of society against cybercrime”.⁷³ While the drafters of the Convention believed that “the introduction and development of effective security measures” was the “most effective means of preventing unauthorised access”, they still made the latter a crime on the ground that “a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage”.⁷⁴ The underlying rationale for criminalizing offenses against the security and integrity of computers was that “[t]echnical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour”.⁷⁵ In the Netherlands, the inclusion of the (later abolished) requirement of infringing a security measure for illegal access “was considered relevant as an incentive to encourage people and companies to protect their computers”.⁷⁶

4.2.3.3 Conflicts with acts, norms and values of hacking

While the Convention’s stated and implied standards and goals represent vital social concerns and public interests and are worthy of promotion and protection as such, they also conflict with and have significant ramifications on both other and others’ norms and values, especially those of hackers who are inevitably affected by computer crime laws. There is no question that the criminalization and prosecution of malicious activities and destructive cyber attacks on com-

⁷² Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 13 and 17.

⁷³ Convention on Cybercrime, Preamble.

⁷⁴ Explanatory Report to the Convention on Cybercrime, para 45.

⁷⁵ Explanatory Report to the Convention on Cybercrime, para 5.

⁷⁶ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 7.

puter systems and data are proper under the law. However, due to the vagueness and overbreadth of the law, the crime of illegal access strikes at the heart of hacking since it broadly prohibits access to and use of computer systems and data and it does not provide adequate exemptions or qualifications for creative and benign forms of hacking.⁷⁷ As previously mentioned, free and open access to information and technology and being able to use them in new, innovative and unexpected ways are conditions and goals of hacking.⁷⁸ But, since hackers can, legally speaking, only enter or access a computer or system that they own or have authority or permission to use (otherwise they may be subject to criminal prosecution), their present and future practices, activities and projects are severely inhibited.⁷⁹ The far-reaching impact of the crime of illegal access on makers and hacktivists is all the more apparent when viewed in light of the six common acts of hacking set forth in Section 1.4.1. Under computer crime laws, hackers are generally forbidden by default to explore or break a computer system without permission even if the aim is to learn how it works. As a consequence, they cannot create new technologies or produce innovations that they can share with others. Furthermore, and here's the rub, by not being able to hack and test a computer system, hackers cannot make it more secure, which ironically is one of the prime objectives of computer crime laws.⁸⁰ Expecting or requiring hackers to seek or obtain prior permission from system owners before they can creatively explore a system is unrealistic given that it is not in their character to ask for permission first before accessing or using technology. In addition, hackers consider requesting *ex ante* permission to be a futile exercise because they believe system owners would refuse their request outright since the latter are generally averse to the discovery of vulnerabilities and weaknesses in their information systems. It must be remembered

⁷⁷ Explanatory Report to the Convention on Cybercrime, para 44.

⁷⁸ See Richard Hollinger, "Hackers: Computer Heroes or Electronic Highwaymen?" 9.

⁷⁹ See Council Directive 2013/40/EU on attacks against information systems, art 2 (d); see Electronic Frontier Foundation, "Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems" 5.

⁸⁰ See Tom Brewster, "US cybercrime law being used to target security researchers".

that it was computer system owners and other private interests who were instrumental in getting computer crime laws passed in the first place.⁸¹ But it should be noted that the attitude of computer owners towards hacking is changing and they are becoming more open to hackers exploring and testing their information systems. This subject is further examined in Section 6.2.1 on responsible disclosure rules and bug bounty programs.

Illegal access also has a detrimental effect on hacker norms and values as set out in Chapter 3. Criminal prosecution, whether threatened or actual, for unauthorized access directly clashes with the norms and values of openness, freedom of access, and freedom of information since computers and knowledge about them are closed off to hackers by default. Further, makers and hacktivists cannot pursue other goals such as curiosity, fun and play, creativity and innovation, transparency, and security since illegal access makes computers black boxes that they cannot freely take apart and explore. It bears repeating that the makers and hacktivists I met generally undertake hacking projects and activities with no malice or intent to cause damage and they do so for the benefit of their community and society as a whole. They are far from being vandals who just want to have fun at someone else's expense. The lack of freedom to access computers has negative effects on hackers' individual autonomy and liberty to follow and develop their own interests, their ability to improve themselves (personal growth), and their positive role and contribution to their communities (community development) and the world at large (social development). As explained in the previous chapters, hackers are socially conscious and have a communitarian ethos, which means that they do not seek personal growth for its own sake but always in relation to how they can contribute to their community and the wider society.

⁸¹ See Helen Nissenbaum, "Hackers and the contested ontology of cyberspace" 202 and 206; see Wayne Rumbles, "Reflections of Hackers in Legal and Popular Discourse" 73; see Reid Skibell, "The Myth of the Computer Hacker" 344.

It is interesting to note that the drafters of the Convention on Cybercrime were quite cognizant that criminalizing mere entry to a computer system would have negative consequences. They acknowledge in the Exploratory Report to the Convention that reservations about or opposition to making access to a computer a crime “stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems”.⁸² The Select Committee of Experts on Computer-related Crime that was originally tasked by the Council of Europe’s European Committee on Crime Problems to study the issue of computer-related crime in the mid to late 1980s had reasonably good knowledge about hacking. In its Recommendation No. R (89) 9 on computer-related crime (Recommendation No. (89) 9), the Committee describes hacker culture in quite a nuanced way:

Hackers explore the capabilities of computers and communications, causing them to perform to their limits.... Pure unauthorised access to computer systems is mainly committed by young hackers, who have a variety of motives. They may intend to improve data protection; they may want to overcome the challenge of a company’s security system; they may enjoy infiltrating data banks, or they may want to boast among friends or to the press. When some cases become public, these acts of hacking can be useful for the detection of loopholes in computer systems.⁸³

However, despite having a fair understanding of hackers, the Committee still recommended the criminalization of unauthorized access because in its words:

the committee considers them as dangerous because system errors, failures, blockades or even crashes may be caused; data may be destroyed by negligence, or security deficiencies, found by acts committed as a challenge, may subsequently be used for financial fraud or for the modification of stored data.... The

⁸² Explanatory Report to the Convention on Cybercrime, para 49.

⁸³ Recommendation No. R (89) 9 on computer-related crime 50; see also Ian Lloyd and Moira Simpson “Computer Crime” in Chris Reed (ed) *Computer Law* 263.

activity of hacking may give access to confidential data which the hacker may use to his own advantage.... In addition, hackers often avoid payments, for example with the aid of so-called 'blue boxes'.⁸⁴

Rather than leaving space for the creative albeit disruptive aspects of hacking, the Committee quite understandably decided on a simpler and more conservative approach. Following the lead and echoing the attitude of the Committee, the drafters of the Convention opted for the broad approach to criminalizing illegal access.⁸⁵

4.2.3.4 Problem of overbreadth and vagueness

Because of the widespread adherence to this broad application and interpretation of the crime of illegal access, it comes as no surprise that, according to legal scholars, the foremost criticisms against the law are that it suffers from overbreadth, vagueness and over-criminalization.⁸⁶ Since the 1980s, the legitimacy, soundness and effectiveness of computer crime laws have been perennially questioned based on these grounds.⁸⁷ The primary reason why computer crime laws, especially the provisions on illegal access, are considered overly broad and vague and that they over-criminalize hacking is because they do not include "subjective criteria" for establishing the mens rea of the proscribed offenses, and thus results in a unreasonably low "threshold for culpability".⁸⁸

A number of early computer crime laws distinguished innocent acts of computer exploration done by well-intentioned hackers

⁸⁴ Recommendation No. R (89) 9 on computer-related crime 50-51.

⁸⁵ Explanatory Report to the Convention on Cybercrime, paras 44 and 49; see also Recommendation No. R (89) 9 on computer-related crime 51.

⁸⁶ Joseph Olivenbaum, "Rethinking Federal Computer Crime Legislation" 604; Orin Kerr, "Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" 1600; Cyrus Chung, "The Computer Fraud and Abuse Act" 242; Reid Skibell, "Cybercrimes & Misdemeanors" 912, 915 and 917; Christine Galbraith, "Access Denied" 358; Cassandra Kirsch, "The Grey Hat Hacker" 394.

⁸⁷ See Reid Skibell, "Cybercrimes & Misdemeanors" 910, 912 and 945; see Samantha Jensen, "Why Broad Interpretations of the CFAA Fail" 98 and 119.

⁸⁸ Recommendation No. R (89) 9 on computer-related crime 53; Reid Skibell, "Cybercrimes & Misdemeanors" 916 and 940

from those harmful activities committed by computer criminals that threatened or caused damage to computer systems and data.⁸⁹ For example, an early California law “criminalized unauthorized access to a computer file made under false pretenses, but excluded actions that were not ‘malicious’ in nature”.⁹⁰ As borne out by the legislative histories of these early US computer crime laws, they were “intended to apply only to crime of computer misuse and not to crimes incidentally involving the use of a computer”.⁹¹ A similar light-touch approach to illegal access was initially considered in other countries. For example, the Scottish Law Commission in the late 1980s recommended the criminalization of illegal access but subject to the condition that the perpetrator had the intention “of procuring an advantage for himself or another person; or of damaging another person’s interest”.⁹² Following this formulation, either a motive of personal gain or an intention to cause damage was a necessary element for the commission of the crime. Thus, for illegal access to be committed, the proposed law would require an ulterior motive or “unauthorised access plus an intent to cause harm to the interests of the computer owner”.⁹³ The rationale for this higher or stricter mens rea standard was to avoid over-criminalization and to ensure that a hacker who gains “access to a system ‘with no intent of abusing its contents and who causes no damage’ would not be held criminally liable.”⁹⁴

However, due to the growing interest and demand by various parties to strengthen and broaden the scope computer crime laws, the subjective criteria of malice or criminal intent was in time either removed from or not incorporated into most computer crime laws,⁹⁵ although some countries such as Austria, Lithuania, Estonia, Hungary,

⁸⁹ Reid Skibell, “Cybercrimes & Misdemeanors” 911 and 912; see Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 104.

⁹⁰ Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 104.

⁹¹ Cyrus Chung, “The Computer Fraud and Abuse Act” 238.

⁹² Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) *Computer Law* 261; see also Recommendation No. R (89) 9 on computer-related crime 51.

⁹³ Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) *Computer Law* 266.

⁹⁴ Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) *Computer Law* 267.

Mexico, Portugal, Romania and Slovakia did include infringing security measures or special or dishonest intent as an additional requirement.⁹⁶ In the United States, a number of states amended their laws to remove the requirement of malicious intent.⁹⁷ Similarly, legislators in the United Kingdom ultimately decided that “the act of obtaining unauthorised access should be made unlawful regardless of whether the perpetrator possessed any ulterior motive” or intended to cause damage.⁹⁸ As a result, certain hacking-related activities “would be declared criminal even where hackers acted out of a sense of curiosity or from the desire to test their computing skills by overcoming security devices intended to prevent unauthorised persons from obtaining access to a computer system”.⁹⁹ Thus, the all-important “legal distinction between benign trespass and harmful cracking has been virtually written out” of the law.¹⁰⁰ The value of reestablishing or setting a higher threshold of culpability through the use of the mens rea standard of malicious intent or “with malice” is proposed and discussed at length in Chapter 6, together with other recommendations on how to improve technology laws and policies related to hacking.

4.2.3.5 Unintended consequences and negative effects

Additionally, the overly broad and vague application and interpretation of the crime of illegal access by public prosecutors, the courts and other authorities have produced further negative knock-on effects in the areas of security, competition and innovation, and the everyday use of technology.¹⁰¹ These “deleterious effects” and unintended consequences of computer crime laws do not only concern or

⁹⁵ Reid Skibell, “Cybercrimes & Misdemeanors” 911; Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 115; see also Recommendation No. R (89) 9 on computer-related crime 49-50.

⁹⁶ Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 14.

⁹⁷ Richard Hollinger and Lonn Lanza-Kaduce, “The Process of Criminalization: The Case of Computer Crime Laws” 115.

⁹⁸ Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) *Computer Law* 261.

⁹⁹ Ian Lloyd and Moira Simpson, “Computer Crime” in C Reed (ed) *Computer Law* 261.

¹⁰⁰ Reid Skibell, “Cybercrimes & Misdemeanors” 921; see also Tom Brewster, “US cybercrime law being used to target security researchers”.

¹⁰¹ Electronic Frontier Foundation, “Let’s Fix Draconian Computer Crime Law”; see also Marcia Hofman and Rainey Reitman, “Re-booting Computer Crime Law Part 1”; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft

impact the purported targets of computer crime laws (i.e., computer criminals and malicious attackers), but they also affect security researchers, market competitors, ordinary users and other actors.¹⁰²

Although counterintuitive, one of the ironic outcomes of criminalizing illegal access is that it ultimately results in making computer systems and data less secure.¹⁰³ In the computer security industry, it is axiomatic that properly securing a system is a difficult and complex matter, and it requires the active involvement of a group of people with deep knowledge of and masterful skills in specific technologies or systems who can rigorously and ingeniously scan, test and attempt to penetrate them – in other words, hackers.¹⁰⁴ The trouble with illegal access is that it makes it risky for hackers to test the security of systems because of the low threshold for committing the offense (i.e., mere access).¹⁰⁵ The law problematically “doesn’t make any distinction between bona fide research and criminal activity”.¹⁰⁶ There have been a number of notable cases and instances where hackers and security researchers have been either threatened with prosecution or actually charged for violating computer crime laws for conducting security research and testing and disclosing information about their findings (see Section 5.2.2.4).¹⁰⁷ Computer crime laws tend to produce a “chilling effect” whereby hackers and “independent researchers around the world working to improve security have faced legal threats under

Directive on Attacks against Computer Systems” 5; see also Zoe Lofgren and Ron Wyden, “Introducing Aaron’s Law”.

¹⁰² Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5; see also Cassandra Kirsch, “The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law” 393-394; see also Samantha Jensen, “Abusing the Computer Fraud and Abuse Act” 116 and 120; see also Christine Galbraith, “Improper use of the Computer Fraud and Abuse Act to Control Information on Publicly

Accessible Internet Websites” 318, 319, 330, 342 and 343; see also Cindy Cohn and Marcia Hoffman, “Rebooting Computer Crime Law Part 2”; see also Adrian Cho, “University Hackers Test the Right To Expose Security Concerns”; see also Hanni Fakhoury, “The U.S. Crackdown on Hackers Is Our New War on Drugs”.

¹⁰³ Reid Skibell, “Cybercrimes & Misdemeanors” 938-939; Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5 and 8.

¹⁰⁴ Cassandra Kirsch, “The Grey Hat Hacker” 396; Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 7; Cindy Cohn and Marcia Hoffman, “Rebooting Computer Crime Law Part 2”.

¹⁰⁵ Tom Brewster, “US cybercrime law being used to target security researchers”; Cassandra Kirsch, “The Grey Hat Hacker” 392.

¹⁰⁶ Tom Brewster, “US cybercrime law being used to target security researchers”.

¹⁰⁷ Lisa O’Carroll, “Scientist banned from revealing codes used to start luxury cars”; see also Adrian Cho, “University Hackers Test the Right To Expose Security Concerns”; see also Tom Brewster, “US cybercrime law being used to target security researchers”; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5, 6 and 8.

existing laws, despite the fact they have no malicious intentions and are performing work that ultimately serves the public”.¹⁰⁸ Society as a whole can benefit from hacking for the purposes of security testing because “there can be very important democratic interests in having access to systems to test for security vulnerabilities even when ‘authorization’ to do so is refused”.¹⁰⁹

Security researchers are not the only ones who are adversely affected by computer crime laws. Companies and commercial enterprises have been threatened or sued for violating the illegal access provision by their market rivals.¹¹⁰ The use of criminal prosecution and the threat of criminal liability as proxies or alternatives to market competition was never the goal or intention of computer crime laws.¹¹¹ Companies particularly those providing internet-based services have used illegal access as a means to impede or “stifle competition” and use the law’s “imprecise language to stymie competitors who create new tools that would spur the economic market and give consumers more choice”. In most of these cases, the acts sought to be suppressed do not infringe or have anything to do with the security of a company’s system.¹¹² The law is merely utilized as an instrument to protect and preserve a perceived competitive advantage, whether it be business, technical or information related.¹¹³ While a person or business has the right resort to any action or remedy that is available to them to seek relief within the bounds of law, what is troubling with these cases is that they are backed by the threat of criminal liability and sanctions,

¹⁰⁸ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5 and 8; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 2, 34 and 51; see also Tom Brewster, “US cybercrime law being used

to target security researchers”; see also Adrian Cho, “University Hackers Test the Right To Expose Security Concerns”.

¹⁰⁹ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 8; see also Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 605.

¹¹⁰ Christine Galbraith, “Access Denied” 318, 319, 330, 333, 342 and 343; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3-4.

¹¹¹ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 4; see also Cindy Cohn and Marcia Hoffman, “Rebooting Computer Crime Law Part 2”.

¹¹² Parker Higgins, “Critical Fixes for the Computer Fraud and Abuse Act”.

¹¹³ Parker Higgins, “Critical Fixes for the Computer Fraud and Abuse Act”.

including imprisonment. It is problematic when computer crime laws are not used to protect the security of computer systems and data, but rather to preserve ways of doing business, which should be generally open to free and robust competition. This misapplication of computer crime laws has a detrimental effect on competition and innovation, which is, again, ironically another primary goal of these laws.¹¹⁴

Ordinary users are also not spared from the negative effects of the legal prohibition against illegal access. Because illegal access is open to expansive interpretation and application by law enforcement bodies and the courts, even the common, everyday practices of ordinary users and their normal uses of technology can be construed as being in violation of the law when coupled with restrictive contracts and terms of service.¹¹⁵ This problem is discussed below in Section 4.4.1.3.

4.2.3.6 Exploitable gaps, loopholes and contradictions

Despite the broad application of the crime of illegal access, it is still possible for makers and hacktivists to engage in hacking activities by taking advantage of a few, small but quite exploitable gaps, loopholes and internal contradictions within the law, whether for tactical purposes or as points of subversion or transformation. Under computer crime laws, it is generally accepted and understood that no criminal liability should attach “for accessing a computer system that permits

¹¹⁴ Convention on Cybercrime, Preamble; Council Directive 2013/40/EU on attacks against information systems, recital 2; see also Cindy Cohn and Marcia Hoffman, “Rebooting Computer Crime Law Part 2”; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 2.

¹¹⁵ Orin Kerr, “Vagueness Challenges to the Computer Fraud and Abuse Act” 1562, 1578, 1579; see also Cyrus Chung, “The Computer Fraud and Abuse Act” 233-234; see also Marcia Hofman and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5; see also Cassandra Kirsch, “The Grey Hat Hacker” 393.

¹¹⁶ Explanatory Report to the Convention on Cybercrime, para 47.

free and open access by the public, as such as is ‘with right’.¹¹⁶ This means that (subject of course to the important assumption or qualification that a mere violation of contractual terms of use is not covered by computer crime laws) there is a general albeit implied permission granted to the public at large to freely access and use publicly available or public-facing computers or systems.¹¹⁷ As such (and assuming there are no inordinately restrictive terms of service), makers and hacktivists have much more leeway to use information and technological products and services that are offered or targeted to the general public such as Facebook, YouTube and Amazon, as well as e-government websites and services since they have been granted authority or permission to use them (in contrast to completely private computer systems). In their roles as users and consumers, makers and hacktivists are afforded certain basic yet quite serviceable rights and protections to engage in hacking projects and activities. Specifically in relation to public websites, internet users (including hackers) have an implicit yet clear right to access and use such websites. As explained by the drafters of the Convention,

the maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself ‘without right’, in particular when the rightholder of the accessed system can be considered to have accepted its application.¹¹⁸

This means that the use of web browsers, “bots”, “crawlers” and other standard or common internet tools, techniques and practices are within the ambit of lawful access, subject of course to technical or contractual stipulations to the contrary (e.g., a prohibition against crawling contained in a robot.txt file).¹¹⁹

¹¹⁷ Christine Galbraith, “Access Denied” 323 and 362; Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 13.

¹¹⁸ Explanatory Report to the Convention on Cybercrime, para 48.

¹¹⁹ Explanatory Report to the Convention on Cybercrime, paras 48 and 58; see also Google, “Crawling & Indexing”; see also M.H.M. Schellekens, “Robot.txt: balancing interests of content producers and content users”; see also Christine Galbraith, “Access Denied” 349-350.

The overriding policy reason and consideration for the preceding gaps and qualifications is that “legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised”.¹²⁰ For instance, the drafters of the Convention were very clear that “the mere sending of an e-mail message or a file to that system” did not amount to illegal access.¹²¹ This restrained approach makes perfect sense because, if one recalls, the essence of computer security crimes like illegal access is to protect against acts that infringe the integrity of computers and data. The drafters of the Convention were quite clear that computer security crimes “are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices”.¹²² This argument is further developed in Section 6.3.1 on ways to improve computer crime laws.

4.2.4. ILLEGAL INTERCEPTION

4.2.4.1 Capture data transmissions and emissions

Illegal interception is the second species of computer security crime. It is perpetrated through the intentional interception “without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data”.¹²³ Interception involves “listening to, monitoring or surveil-

¹²⁰ Explanatory Report to the Convention on Cybercrime, para 38 (emphasis added).

¹²¹ Explanatory Report to the Convention on Cybercrime, para 46; but see Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 10 (it is subject to specific anti-spam laws); see also Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 6.

¹²² Explanatory Report to the Convention on Cybercrime, para 43.

¹²³ Convention on Cybercrime, art 3; see also Council Directive 2013/40/EU on attacks against information systems, art 6; see also Recommendation No. R (89) 9 on computer-related crime 54 and 55.

¹²⁴ Explanatory Report to the Convention on Cybercrime, para 53; see also Council Directive 2013/40/EU on attacks against information systems, recital 9 (for a more detailed definition).

lance of the content” of both inter- and intra-computer communications.¹²⁴ It can be accomplished either “directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means”.¹²⁵ The phrase “transmissions of computer data” covers “all forms of electronic data transfers, whether by telephone, fax, e-mail or file transfer”.¹²⁶ Under the law, interception through “technical means” may be done through the use of a computer system, “electronic eavesdropping or tapping devices.... technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes” including “spyware and surveillance software”.¹²⁷

The crime of illegal interception prohibits the tapping, eavesdropping or recording of both electronic data transmissions and emissions.¹²⁸ It also applies to the unauthorized capturing of “data between computer and keyboard or of residual radiation from a computer screen”.¹²⁹ The interception of electromagnetic emissions, “radiation and electronic fields surrounding the computer (terminal), for example for display on the eavesdropper’s screen”,¹³⁰ is popularly known as “van Eck phreaking”. This process is named after a Dutch researcher who published a paper on the possibility of monitoring information displayed on a video terminal (even from as far away as 1 kilometer) by “picking up and decoding the electromagnetic interferences” and emissions that it produced and reconstructing the data on a normal TV receiver.¹³¹ Aside from computers, other parts and

¹²⁵ Council Directive 2013/40/EU on attacks against information systems, recital 9; see also Recommendation No. R (89) 9 on computer-related crime 54.

¹²⁶ Explanatory Report to the Convention on Cybercrime, para 52.

¹²⁷ Explanatory Report to the Convention on Cybercrime, para 53; David Wall, *Cybercrime* 59 and 60; see also Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 6 (spyware is “software that is installed on a user’s computer without his knowledge. Such software transmits information on the user and his habits once connected to the internet. The information gathered this way is usually intended for use by advertisers”).

¹²⁸ Recommendation No. R (89) 9 on computer-related crime 53.

¹²⁹ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8.

¹³⁰ Recommendation No. R (89) 9 on computer-related crime 53.

¹³¹ Wim van Eck, “Electromagnetic Radiation from Video Display Units” 269 and 276; see also Robert Gehling, Ryan Ashley and Thomas Griffin, “Electronic Emissions Security” 306 (for more information on emissions security).

components of an information system that emit or leak electromagnetic emissions as part of their normal operations include power cables, computer and network cables, power lines, cable TV, wireless access points, and even metal desks and metal ducts and pipes.¹³² It is worth pointing out that van Eck phreaking (alternatively called a TEMPEST attack) was utilized during the successful hacking of electronic voting machines in the Netherlands in 2006, which resulted in the latter's withdrawal from use in Dutch elections.¹³³ This case will be discussed in depth in Section 5.2.2.2.

There are various ways to intercept electronic communications and transmissions. Two popular means are keystroke logging and man-in-the-middle attacks. Keystroke logging is accomplished when an attacker installs on target computers a "keylogger" program that monitors and captures users' keystrokes without their knowledge, and then storing or sending the information back to the attacker for reconstruction and analysis.¹³⁴ There is a natural connection between illegal access and illegal interception since gaining physical or electronic access to a target computer is normally a prerequisite for the installation of a keylogger, and the intercepted data is often used to access other computers and systems.¹³⁵ Interception can also be done through a man-in-the-middle attack.¹³⁶ Attackers can insinuate themselves or their devices between two communicating computers and then capture data being sent between the two without the communicating parties noticing.¹³⁷ This is often done by hijacking or impersonating an intermediate communications device (e.g., a WiFi router or a cellular access

¹³² Robert Gehling, Ryan Ashley and Thomas Griffin, "Electronic Emissions Security" 306, 307 and 308.

¹³³ Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands: from early Adoption to early Abolishment" 11; see Robert Gehling, Ryan Ashley and Thomas Griffin, "Electronic Emissions Security" 307-308 (for a discussion of TEMPEST)

¹³⁴ David Wall, *Cybercrime* 60.

¹³⁵ See Explanatory Report to the Convention on Cybercrime, para 59.

¹³⁶ See Ryan Iwahashi, "How to Circumvent Technology Protection Measures Without Violating the DMCA" 508-509.

¹³⁷ See Jeffrey Bardzell, "Virtual Worlds and Fraud" 746.

point) or a computer server or network used by the target parties.

4.2.4.2 Legal and social justification

In addition to the three main objectives of computer security crime (i.e., deterrence, technology development, and security), the criminalization of illegal interception is also meant to extend the protection of the right to privacy of communications and correspondence to digital communications.¹³⁸ Infringing the secrecy and confidentiality of communications is therefore the gist of the offense.¹³⁹ As the drafters of the Convention explain, the term “‘non-public’ qualifies the nature of the transmission (communication) process and not the nature of the data transmitted.... The term ‘non public’ does not per se exclude communications via public networks”.¹⁴⁰

Compared to illegal access, illegal interception is not as highly problematic for makers and hackers. For one, the act of illegal interception is more narrowly and clearly delimited. For example, “the use of common commercial practices, such as employing ‘cookies’, is not intended to be criminalised as such, as not being an interception ‘without right’”.¹⁴¹ Likewise, as explicitly stated by the drafters of the Convention, even though radio connections are technically covered, it is not a crime to intercept “any radio transmission which, even though ‘non public’, takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs”.¹⁴² In order to further delimit the scope of illegal access, the drafters of the Convention also included the requirement of “technical means” as “a restrictive qualification to avoid over-criminalisation”.¹⁴³

It bears pointing out that, unless interception is absolutely

¹³⁸ Explanatory Report to the Convention on Cybercrime, para 51; Recommendation No. R (89) 9 on computer-related crime 53.

¹³⁹ Recommendation No. R (89) 9 on computer-related crime 54.

¹⁴⁰ Explanatory Report to the Convention on Cybercrime, para 54.

¹⁴¹ Explanatory Report to the Convention on Cybercrime, para 58.

¹⁴² Explanatory Report to the Convention on Cybercrime, para 56.

¹⁴³ Explanatory Report to the Convention on Cybercrime, para 53; Recommendation No. R (89) 9 on computer-related crime 54.

necessary to gain access to or use of a system or to test its security (which is seldom the case), makers and hackers generally do not need nor want to intercept electronic communications. As shown in Section 3.4.6.4, makers and hackers place great value on their and others people's privacy, particularly the confidentiality and secrecy of communications and correspondence.¹⁴⁴ Despite a number of high profile data privacy breaches committed by some hackers,¹⁴⁵ makers and hackers on the whole consider privacy to be a paramount norm and value that needs to be vigorously upheld and protected, mainly through the development, distribution and use of privacy-enhancing technologies.¹⁴⁶

4.2.5 DATA INTERFERENCE AND SYSTEM INTERFERENCE

4.2.5.1 Damage or hinder computer data and systems

The third and fourth kinds of computer security crime are data interference and system interference. Because of their conceptual and practical connections and the “great similarity to the legal interests” that they seek to protect, it makes sense to examine them together.¹⁴⁷ Data interference involves the intentional “damaging, deletion, deterioration, alteration or suppression of computer data without right”.¹⁴⁸ In the Cybercrime Directive, the phrase “or by rendering such data inaccessible” has been incorporated in the definition of the offense. It is worth pointing out that, because of the many possible reasons or motivations for a person to damage computer data (e.g., for profit or

¹⁴⁴ Chaos Computer Club, “hackerethics”; see Eric Hughes, “A Cypherpunk’s Manifesto”; see Julian Assange and others, Cypherpunks.

¹⁴⁵ See Verizon, “2012 Data Breach Investigations Report” 15, 19 and 20; Verizon, “2012 Data Breach Investigations Report” 4 and 6; Ingrid Lunden, “Hacktivists To Blame for 58 Percent of Stolen Data In 2011, Says Verizon Study”; E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”.

¹⁴⁶ See Tim Jordan, *Activism!* 127; see Julian Assange and others, Cypherpunks; see Bits of Freedom, “Internet-freedom Toolbox” <<https://www.bof.nl/ons-werk/internetvrijheid-toolbox/>> accessed 29 July 2015; see Open Technology Fund, “Projects” <<https://www.opentechfund.org/projects/>>; see Tactical Technology Collective, “Security in-a-box” <<https://tacticaltech.org/projects/security-box/>> accessed 29 July 2015; see Riseup <<https://help.riseup.net/>> accessed 29 July 2015; see Electronic Frontier Foundation, “Surveillance Self-Defense” <<https://ssd.eff.org/en/>> accessed 29 July 2015.

personal gain, revenge, political or ideological reasons, or public attention), the Select Committee of Experts on Computer-related Crime thought it best that the offense of data interference should pertain specifically to computer data and programs rather than the entire information system. Their rationale for this was that “referring to the act and its immediate effect on the software or the stored data rather than to remote consequences for the whole system is preferable in order to effectively protect such software and the data concerned from mischievous damage and interference”.¹⁴⁹ As further explained by the Committee

The specific character of damage done to data means that... it is not a matter of injuring the substance of the object and thus impairing its utilisation but rather a matter of altering the quality of the information in stored data and programs, which may obviously reduce their potential use”.¹⁵⁰

Physical damage to the information system is not required.¹⁵¹ It should be noted that the prohibited act of data interference affects both the quantitative and qualitative aspects of a computer program or data.¹⁵² In addition, “[d]ata and programs are protected in different stages, regardless of whether they are stored, processed or transferred by means of computer-automated equipment”.¹⁵³ For its part, system interference is intentionally causing “the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data”.¹⁵⁴ The Cybercrime Directive also adds the requisites of

¹⁴⁷ Recommendation No. R (89) 9 on computer-related crime 46 and 48.

¹⁴⁸ Convention on Cybercrime, art 4 para 1; see also Recommendation No. R (89) 9 on computer-related crime 44.

¹⁴⁹ Recommendation No. R (89) 9 on computer-related crime 43; see also Explanatory Report to the Convention on Cybercrime, para 65.

¹⁵⁰ Recommendation No. R (89) 9 on computer-related crime 44.

¹⁵¹ Xiang Li, “Hacktivism and the First Amendment” 311; see Explanatory Report to the Convention on Cybercrime, para 60; see Recommendation No. R (89) 9 on computer-related crime 45.

¹⁵² Recommendation No. R (89) 9 on computer-related crime 44; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 19.

¹⁵³ Recommendation No. R (89) 9 on computer-related crime 45.

¹⁵⁴ Convention on Cybercrime, art 5; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 22.

¹⁵⁵ Council Directive 2013/40/EU on attacks against information systems, art 4 (emphasis added).

¹⁵⁶ Explanatory Report to the Convention on Cybercrime, para 65; see Recommendation No. R (89) 9 on computer-related crime 46.

“seriously hindering or interrupting”.¹⁵⁵ The offence of system interference is also called “computer sabotage”.¹⁵⁶

Under the Convention on Cybercrime, the terms “damaging” and “deterioration” concern the “negative alteration of the integrity or of information content of data and programmes”.¹⁵⁷ The act of “deletion” involves destroying data and making it unrecognizable.¹⁵⁸ “Alteration” is about the change or “modification of existing data” in such a way that “it changes the informational quality of the data or programs, usually to the disadvantage of the person concerned”.¹⁵⁹ Alteration also covers the “[t]he input of malicious codes, such as viruses and Trojan horses... as is the resulting modification of the data”.¹⁶⁰ Under Dutch law, “adding data” is expressly included in the list of prohibited acts because, while the act “does not interfere with existing data as such, it does interfere with the integrity of documents or folders, so that it can be seen as a more abstract form of data interference”.¹⁶¹ “Suppression” pertains to “any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored”.¹⁶² Technically, a person can be held liable for the crime of data interference for any unauthorized change of data. Under Dutch law, “[t]here is no threshold – even unlawfully changing a single bit is an offense”.¹⁶³ While the interference must be done intentionally, under Dutch law, a person can also be held liable for data interference through negligence “if serious damage is caused”.¹⁶⁴

¹⁵⁷ Explanatory Report to the Convention on Cybercrime, para 61; see also Recommendation No. R (89) 9 on computer-related crime 45.

¹⁵⁸ Explanatory Report to the Convention on Cybercrime, para 61; Recommendation No. R (89) 9 on computer-related crime 45.

¹⁵⁹ Explanatory Report to the Convention on Cybercrime, para 61; Recommendation No. R (89) 9 on computer-related crime 61.

¹⁶⁰ Explanatory Report to the Convention on Cybercrime, para 61; Recommendation No. R (89) 9 on computer-related crime 60-61.

¹⁶¹ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8.

¹⁶² Explanatory Report to the Convention on Cybercrime, para 61; see also Recommendation No. R (89) 9 on computer-related crime 45.

¹⁶³ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8 (but this is subject to the prosecutorial discretion of the public prosecutor).

¹⁶⁴ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8; see also Explanatory Report to the Convention on Cybercrime, para 63.

In relation to system interference, “hindering refers to actions that interfere with the proper functioning of a computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data”.¹⁶⁵ According to the drafters of the Convention, “functioning” should be understood in a technologically neutral way, and thus covers and protects “all kinds of functions” of “all kinds” of computers and telecommunications systems.¹⁶⁶ A further requisite of the offense of system interference is that the hindering must be “serious”.¹⁶⁷ The requirement of seriousness is meant to prevent over-criminalization.¹⁶⁸ While the prerogative and responsibility of defining what serious means falls on state parties, the drafters of the Convention consider the following examples serious interference: “the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems”.¹⁶⁹ Under Dutch law, for example, there is serious damage when a computer system is not “available for several hours”.¹⁷⁰ As with data interference, in Dutch law, system interference can also be committed through negligent acts.¹⁷¹

The main legal interest sought to be protected by the criminalization of data and system interference is “the integrity and proper functioning or use of stored computer data or computer programs”.¹⁷² On its face, the law appears to be solely concerned with the rights

¹⁶⁵ Explanatory Report to the Convention on Cybercrime, para 66; Recommendation No. R (89) 9 on computer-related crime 49; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 20.

¹⁶⁶ Explanatory Report to the Convention on Cybercrime, para 65; Recommendation No. R (89) 9 on computer-related crime 48 and 49.

¹⁶⁷ Explanatory Report to the Convention on Cybercrime, para 67; Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 23.

¹⁶⁸ Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 23.

¹⁶⁹ Explanatory Report to the Convention on Cybercrime, para 67; see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 20.

¹⁷⁰ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8.

¹⁷¹ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 9.

¹⁷² Explanatory Report to the Convention on Cybercrime, paras 60 and 65; see also Recommendation No. R (89) 9 on computer-related crime 44.

¹⁷³ Recommendation No. R (89) 9 on computer-related crime 47; see also Explanatory Report to the Convention on Cybercrime, para 65.

and interests of the owners, operators or users of computer data and systems.¹⁷³ But, as Recommendation No. (89) 9 states, “the protection of the functioning of the systems is of great interest not only to the owners/users of them, but in many cases also to the public”.¹⁷⁴ In addition to the substantial economic value of information systems and the considerable loss that would be incurred in cases of harm or damage to them, data and system interference “may not only have great economic consequences, but may also lead to disastrous human consequences”.¹⁷⁵ As such, the “proper functioning of companies and organisations as well as of social processes is particularly at stake here”.¹⁷⁶ In line with this, the law seeks to promote other social goals or values like “combating organised crime, increasing the resilience of computer networks, protecting critical information infrastructure and data protection”.¹⁷⁷

4.2.5.2 Cyber attacks as a form of system interference

One of the primary objectives of the Cybercrime Directive is to combat the growing number and intensity of “large-scale cyber attacks” that cause serious data and system interference.¹⁷⁸ Specifically, the Directive aims to introduce and impose “criminal penalties for the creation of botnets”.¹⁷⁹ A botnet is “a network of computers that have been infected by malicious software (computer virus)”.¹⁸⁰

Such network of compromised computers (‘zombies’) may be activated to perform specific actions such as attacks against information systems (cyber-attacks). These ‘zombies’ can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This ‘controlling’ computer is also known as the ‘command-and-control centre’.

¹⁷⁴ Recommendation No. R (89) 9 on computer-related crime 46.

¹⁷⁵ Recommendation No. R (89) 9 on computer-related crime 43 and 46.

¹⁷⁶ Recommendation No. R (89) 9 on computer-related crime 43.

¹⁷⁷ Commission, “Proposal for a Directive on attacks against information systems” COM(2010) 517, 4.

¹⁷⁸ Council Directive 2013/40/EU on attacks against information systems, recitals 5, 6, 13 and 26; see also Commission, “Proposal for a Directive on attacks against information systems” COM(2010) 517, 3.

¹⁷⁹ Council Directive 2013/40/EU on attacks against information systems, recital 5.

¹⁸⁰ Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 1 and 5.

The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack, might be located elsewhere than the offender himself.¹⁸¹

Botnets are often used to carry out denial-of-service (DoS) attacks, which is an “assault on a network that floods it with so many requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a DoS attack interrupts network service for some period”.¹⁸² A distribute denial-of-service (DDoS) attack is one that employs a “big botnet” of hundreds or thousands of zombie computers that can “cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc.”¹⁸³ While there are various ways and different motivations for conducting DDoS attacks, overall they are “largely characterized by massive participation, disruption of communications and reliance on the net’s structural vulnerabilities”.¹⁸⁴

The Directive is also particularly concerned with protecting “critical infrastructure” related to computer and telecommunications systems, which is “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people..., and the disruption or destruction of which would have a significant impact”.¹⁸⁵ According to the European Commission, these large-scale cyber attacks “pose a serious risk to public interests” because they can cause “serious damage”.¹⁸⁶ While the Directive allows Member States

¹⁸¹ Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 5.

¹⁸² Computer Desktop Encyclopedia; see also Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 5; see also Andrew Chadwick, *Internet Politics* 130; see also Xiang Li, “Hacktivism and the First Amendment” 306-307; Tim Jordan, *Activism!* 124; Argyro Karanasiou, “The changing face of protests in the digital age” 100.

¹⁸³ Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 5; see also Xiang Li, “Hacktivism and the First Amendment” 307; see also Argyro Karanasiou, “The changing face of protests in the digital age” 100.

¹⁸⁴ Argyro Karanasiou, “The changing face of protests in the digital age” 100; see also Noah Hampson, “Hacktivism” 532.

¹⁸⁵ Council Directive 2013/40/EU on attacks against information systems, recital 4.

¹⁸⁶ Council Directive 2013/40/EU on attacks against information systems, recital 5.

to “determine what constitutes serious damage”, illustrative examples include “disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information”.¹⁸⁷

Aside from DDoS attacks, other common activities or technologies that may be used to damage computer data or seriously hinder the functioning of information systems include spam attacks¹⁸⁸ and malware¹⁸⁹ such as computer viruses,¹⁹⁰ worms,¹⁹¹ trojans,¹⁹² back doors,¹⁹³ and logic bombs.¹⁹⁴

4.2.5.3 Lawful versus unlawful interference

The offenses of data and system interference are generally not pertinent or applicable to makers. Makers generally do not need to change or interfere with other people’s computer data or systems in order to build or work on their projects. They legitimately own, buy, possess or create the information or technologies that they hack and thus have the rights to access and use them. The most disruptive activity they may engage in is reverse engineering, which is a legally permitted under certain conditions (see Section 4.3.3.1 below).¹⁹⁵ In

¹⁸⁷ Council Directive 2013/40/EU on attacks against information systems, recital 5.

¹⁸⁸ Andrew Chadwick, *Internet Politics* 130 (also called “email bombing”, this type of attack utilizes “automation software to inundate an email mailbox... with the aim of crippling an organization’s email capabilities”); see also Lorenzo Picotti and Ivan Salvadori, “National legislation implementing the Convention on Cybercrime” 23.

¹⁸⁹ Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 5 (a contraction of malicious software, malware is “computer software designed to infiltrate or damage or computer system without the owner’s consent. It is distributed through a variety of means (emails, computer viruses, and botnets)”); see also Andrew Chadwick, *Internet Politics* 130.

¹⁹⁰ A virus is a computer program that “copies itself to other programs in the computer and other computers in the network” (Computer Desktop Encyclopedia); see also Recommendation No. R (89) 9 on computer-related crime 43.

¹⁹¹ A “worm” is a “destructive program that replicates itself throughout a single computer or across a network, both wired and wireless. It can do damage by sheer reproduction, consuming internal disk and memory resources within a single computer or by exhausting network bandwidth” (Computer Desktop Encyclopedia).

¹⁹² A “trojan” is “similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control over the computer” by creating a back door (Computer Desktop Encyclopedia).

¹⁹³ A “back door” is “a secret way to take control of a computer” that allows someone to gain access to a computer or software and “activate either normal or hidden functions” (Computer Desktop Encyclopedia).

¹⁹⁴ A “logic bomb” is “a program routine that destroys data when certain conditions are met” (Computer Desktop Encyclopedia); see also Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013, 5; see also Explanatory Report to the Convention on Cybercrime, para 67 and 68; see also Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 8-9; see also Recommendation No. R (89) 9 on computer-related crime 43; see also Xiang Li, “Hacktivism and the First Amendment” 311; Argyro Karanasiou, “The changing face of protests in the digital age” 101 (citing Samuel).

¹⁹⁵ See Directive 2009/24/EC on the legal protection of computer programs.

contrast, hacktivists find themselves squarely in the crosshairs of the law because they tend to engage in more radical and disruptive acts of cyber protests and electronic civil disobedience to advance their socio-political causes and campaigns.¹⁹⁶

Hactivist groups like Anonymous typically resort to DDoS attacks,¹⁹⁷ website defacements,¹⁹⁸ site redirects,¹⁹⁹ ping storms,²⁰⁰ and breaking into systems to obtain data and then making the data public.²⁰¹ Pursuant to computer crime laws, engaging in these types of activities exposes the attackers to criminal liability for data and system interference whether they are cybercriminals doing it for fraudulent purposes or personal gain, or hacktivists endeavoring to achieve a higher goal or social value.²⁰² There is, however, a debate as to whether aggressive and transgressive acts of hacktivism should be recognized and protected under the law as legitimate forms of cyber protests or electronic civil disobedience.²⁰³ Although nothing further came out of it, Anonymous even filed a formal public petition on the US whitehouse.gov website asking that DDoS attacks carried out by hacktivists be recognized as lawful protests and not subject to criminal prosecution.²⁰⁴ There is some basis for conceiving of hacktivism as the digital equivalent of street protests. As Li explains, hacktivists and traditional protesters have similar motivations, desire to bring as much public-

¹⁹⁶ Andrew Chadwick, *Internet Politics* 130; Xiang Li, "Hacktivism and the First Amendment" 310-311; Noah Hampson, "Hacktivism" 514 and 520.

¹⁹⁷ E. Gabriella Coleman, "Anonymous: From the Lulz to Collective Action".

¹⁹⁸ Andrew Chadwick, *Internet Politics* 130 (considered the "the most common form of hacktivism", it is carried out by "breaking into and altering the content of a website to change its content"); see also Xiang Li, "Hacktivism and the First Amendment" 307; Noah Hampson, "Hacktivism" 519.

¹⁹⁹ "Hacktivism and the First Amendment" 307 ("hacking into the web server and altering the address settings to redirect visitors to a different website"); see also Andrew Chadwick, *Internet Politics* 130 (the act of "intercepting web traffic destined for a particular site and redirecting it elsewhere").

²⁰⁰ Andrew Chadwick, *Internet Politics* 130 ("uses the Internet 'ping' program (used to test the presence of a computer on a network) to overload a server by flooding it with 'ping' requests").

²⁰¹ Xiang Li, "Hacktivism and the First Amendment" 308 ("hacking into a private network and stealing information or data. Publication or release of the stolen data sometimes follows the attack.").

²⁰² Argyro Karanasiou, "The changing face of protests in the digital age" 99 and 100.

²⁰³ See Mathias Klang, "Civil Disobedience Online"; see Xiang Li, "Hacktivism and the First Amendment" 304; Tim Jordan, *Activism!* 127 ("a new class of civil disobedience"); see Argyro Karanasiou, "The changing face of protests in the digital age" 99, 101 and 107.

²⁰⁴ Xiang Li, "Hacktivism and the First Amendment" 304 (but the petition did not progress because "it failed to meet the signature threshold" that was "required to guarantee a White house response"); see also Argyro Karanasiou, "The changing face of protests in the digital age" 99.

ty and attention to their campaigns and protest actions, and, as they engage in mass actions, they need to mobilize and mass their presence and numbers at a specific place and time to get as much impact and attention from the target of the protest, as well as the general or relevant public.²⁰⁵ Hackivism and traditional protests are alike in that they both aim “to effect political or social change, often in response to a particular political or social event”.²⁰⁶ Hacktivists, for instance, have undertaken DDoS attacks against repressive foreign governments, site redirects against racist groups, and website defacements that parody government officials.²⁰⁷

But attempts to equate cyber protests with traditional mass actions (and the applicability of consequent legal protections afforded to the latter) have been disputed on a number of grounds.²⁰⁸ First of all, the rights to assemble and protests are not absolute whether in the physical or virtual world, and they are subject to reasonable regulation. Further, under US law, it is believed that “[h]ackivism that causes damage (for example, information theft) or involves the manipulation of hijacked private property (for example, DDoS attacks using involuntary botnets) therefore is not likely to be considered expression at all”.²⁰⁹ Across the pond, Hampson holds a similar view: “It would not be surprising if British courts refused to recognize a free speech exception to the CMA [Computer Misuse Act] for hacktivism, even under the HRA [Human Rights Act]”.²¹⁰ One of the strongest arguments against granting legitimacy to certain forms of hacktivism like DDoS attacks is that

²⁰⁵ Xiang Li, “Hacktivism and the First Amendment” 308, 309 and 324; Tim Jordan, *Activism!* 124; Argyro Karanasiou, “The changing face of protests in the digital age” 104.

²⁰⁶ Xiang Li, “Hacktivism and the First Amendment” 308; see also Mathias Klang, “Civil Disobedience Online” 7-8; see also Argyro Karanasiou, “The changing face of protests in the digital age” 103.

²⁰⁷ Paul Taylor, “Editorial: Hacktivism”; Andrew Chadwick, *Internet Politics* 131-132; Seth Kreimer, “Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet” 156-157; Peter Ludlow, “WikiLeaks and Hacktivist Culture” 26.

²⁰⁸ See Joshua McLaurin, “Making Cyberspace Safe for Democracy”.

²⁰⁹ Noah Hampson, “Hacktivism: A New Bread of Protest in a Networked World” 533; see also Joshua McLaurin, “Making Cyberspace Safe for Democracy” 236.

²¹⁰ Noah Hampson, “Hacktivism: A New Bread of Protest in a Networked World” 535.

²¹¹ Xiang Li, “Hacktivism and the First Amendment” 322; see also Tim Jordan, *Activism!* 126; see also Jennifer Chandler, “Security in Cyberspace: Combatting Distributed Denial of Service Attacks” 240; see also Argyro Karanasiou, “The changing face of protests in the digital age” 108.

the latter are “censorial in nature” and, thus, not worthy of legal much less constitutional protection.²¹¹ The reasoning behind this is that if “the information posted on a website constitutes speech by another party”, then attacking or interrupting the target websites results in the muzzling or censorship of others.²¹² Furthermore, since a website is someone else’s private property, “a hacktivist has no... right to exercise speech ‘on’ another’s website”,²¹³ and “the law... does not protect speech on private property against the wishes of the owner”.²¹⁴ Jordan similarly opines that a DDoS attack “is the restraint of information, the jamming and prevention of someone contributing to or receiving information, by preventing their website or Internet connections from working”.²¹⁵ There is even disagreement among hacktivists about the propriety of DDoS attacks.²¹⁶ Oxblood Ruffin of the hacker group Cult of the Dead Cow is emphatic about his disapproval:

Denial of Service attacks are a violation of the First Amendment, and of the freedoms of expression and assembly. No rationale, even in the service of the highest ideals, makes them anything other than what they are – illegal, unethical, and uncivil. One does not make a better point in a public forum by shouting down one’s opponent. Say something more intelligent or observe your opponents’ technology and leverage your assets against them in creative and legal ways.²¹⁷

It may also be said that the level and extent of disruption caused by DDoS attacks are highly disproportionate because it is one of “the most destructive of all available means of getting a message across online”.²¹⁸ There is sufficient legal basis then to conclude that

²¹² Xiang Li, “Hacktivism and the First Amendment” 321 and 322; see also Jennifer Chandler, “Security in Cyberspace: Combatting Distributed Denial of Service Attacks” 240.

²¹³ Xiang Li, “Hacktivism and the First Amendment” 323; see also Argyro Karanasiou, “The changing face of protests in the digital age” 105 and 107.

²¹⁴ Xiang Li, “Hacktivism and the First Amendment” 313; see also Mathias Klang, “Civil Disobedience Online” 8.

²¹⁵ Tim Jordan, *Activism!* 133-134; Xiang Li, “Hacktivism and the First Amendment” 321.

²¹⁶ Kirsty Best, “Visceral Hacking or Packet Wanking? The Ethics of Digital Code” 229.

²¹⁷ Oxblood Ruffin, “Hacktivism”.

²¹⁸ Argyro Karanasiou, “The changing face of protests in the digital age” 105, 106 and 109.

²¹⁹ Xiang Li, “Hacktivism and the First Amendment” 316 and 318; see also Joshua McLaurin, “Making Cyberspace Safe for Democracy” 246.

DDoS attacks “against privately created websites are unlikely to qualify for constitutional protection”²¹⁹ since they “are mere conduct, devoid of expression because a downed website does not communicate the content of any intended message”.²²⁰ Moreover, as with website defacements, site redirects and ping storms, “it is unlikely that information theft or virtual sabotage qualify as symbolic speech” that would benefit from legal protection.²²¹ Based on the law as it currently stands, there seems to be a legal consensus and social agreement that certain extreme forms of cyber protests such as DDoS attacks are not constitutionally protected speech or activities, and are punishable under computer crime laws.²²²

In addition, hacktivism has been accused of suffering from certain democratic deficiencies.²²³ First of all, the voluntary nature of cyber protests has been called into question, especially in cases where computers of ordinary users were co-opted to form part of a botnet without their knowledge or consent.²²⁴ Second, the argument that cyber protests are lawful mass and direct actions of citizens is severely weakened because the use of increasingly effective and sophisticated technologies often means that less people are required to carry them out.²²⁵ The paradoxical results of making technology a central and considerable part of protest actions is that it “cuts in two separate ways: (1) technology lowers the barriers to participation, and (2) fewer active participants are required to execute an effective cyberattack (as compared with a traditional protest)”.²²⁶ Because there is less engagement of and by the public, it is thus harder to justify cyber protests as

²²⁰ Xiang Li, “Hacktivism and the First Amendment” 321.

²²¹ Xiang Li, “Hacktivism and the First Amendment” 320 and 321; see also Tim Jordan, *Activism!* 127; see also Noah Hampson, “Hacktivism” 537; see also Argyro Karanasiou, “The changing face of protests in the digital age” 105.

²²² See Joshua McLaurin, “Making Cyberspace Safe for Democracy” 2456; see Noah Hampson, “Hacktivism: A New Bread of Protest in a Networked World” 537; see Argyro Karanasiou, “The changing face of protests in the digital age” 107; see Kenneth Einar Himma, “Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?” 22; see Mathias Klang, “Civil Disobedience Online” 4 and 7; see Xiang Li, “Hacktivism and the First Amendment”; see Seth Kreimer, “Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet” 158.

²²³ Xiang Li, “Hacktivism and the First Amendment” 309.

²²⁴ Xiang Li, “Hacktivism and the First Amendment” 309.

²²⁵ Xiang Li, “Hacktivism and the First Amendment” 309; Oxblood Ruffin, “Hacktivism”.

²²⁶ Xiang Li, “Hacktivism and the First Amendment” 309; see also Oxblood Ruffin, “Hacktivism”.

²²⁷ Joshua McLaurin, “Making Cyberspace Safe for Democracy” 245; see also Oxblood Ruffin, “Hacktivism”.

the will of the people as opposed to being the actions of a minority. Finally, there have been some misgivings about the level of commitment and actual participation of some hacktivists.²²⁷ As Li points out,

when compared with traditional protests, cyberattacks are less costly to execute in terms of actual resources as well as physical effort and public presence.... while traditional protests are accomplished through picketing, marches, or public sit-ins, hacktivism is accomplished through a variety of digital tools, often from behind a computer screen.²²⁸

Since many forms of hacktivism are conducted anonymously and in relative isolation, there is in certain cases “low personal cost assumed by the participants”.²²⁹ Because of the low barrier for participation and the presumed lower risks involved, it may be said that an act of hacktivism, “which does not incur any significant personal cost for the participants, takes away the element of a public act, normally met in acts of civil disobedience”.²³⁰ Unlike street protests, hacktivists also find it much harder to feel or build a sense of solidarity to their cause.²³¹

Despite the above legal and social criticisms of hacktivism, it should be borne in mind that not all acts of hacktivism and the consequent data and system interference that they produce are negative or destructive. In fact, hacktivism can produce positive effects and can be quite constructive. Hacktivists have played a significant role in many socio-political protests, movements and even revolutions around the world.²³² While their participation is mostly confined to the technical matters, hacktivists have made valuable contributions to diverse

²²⁸ Xiang Li, “Hacktivism and the First Amendment” 309.

²²⁹ Argyro Karanasiou, “The changing face of protests in the digital age” 101; see also Noah Hampson, “Hacktivism” 541.

²³⁰ Argyro Karanasiou, “The changing face of protests in the digital age” 101 and 102.

²³¹ Tim Jordan, *Activism!* 125.

²³² Tim Jordan, *Activism!* 122-123; Paul Taylor, “Editorial: Hacktivism”; Andrew Chadwick, *Internet Politics* 131-132; E. Gabriella Coleman, “Anonymous: From the Lulz to Collective Action”.

²³³ Paul Taylor, “Editorial: Hacktivism”; Andrew Chadwick, *Internet Politics* 131-132; Peter Ludlow, “WikiLeaks and Hacktivist Culture” 26.

actions and causes.²³³ For instance, Anonymous provided protesters in Tunisia with technical assistance, instructions and tools to circumvent government surveillance and internet blockages during the Arab Spring.²³⁴ Hacktivists also produce and use computer programs and devices for themselves and others to bypass firewalls and other technical restrictions to the free flow of information and route around government censorship and filtering.²³⁵ They may also hack information systems to bring attention to security weaknesses and not to exploit the discovered vulnerabilities.²³⁶ After Edward Snowden's revelations in 2013 of the US government's global electronic surveillance operations, hacktivists and other types of hackers have been mustering and concentrating their efforts and resources toward developing better encryption, anonymizing and other security and privacy-enhancing technologies that everyone (especially ordinary citizens and users) can freely access and use to protect their privacy and security both online and offline.²³⁷ It is interesting to note that most if not all of the software that hacktivists create (e.g., the Low Orbit Ion Cannon (LOIC for short) that members of Anonymous used in high-profile DDoS attacks in support of WikiLeaks) are either licensed as free and open source software (FOSS) or released as public domain works online, and are thus publicly available to and freely modifiable by anyone who has internet access.²³⁸

Some hacktivists even intentionally choose to be less dependent and reliant on the power and efficiencies offered by technology in order not to cause damage or permanent disruption.²³⁹ For example,

²³⁴ E. Gabriella Coleman, "Anonymous: From the Lulz to Collective Action".

²³⁵ Tim Jordan, *Activism!* 128-129; Electronic Frontier Foundation, "Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems" 9.

²³⁶ Tim Jordan, *Activism!* 130-131.

²³⁷ See Bits of Freedom, "Internet-freedom Toolbox" <<https://www.bof.nl/ons-werk/internetvrijheid-toolbox/>> accessed 29 July 2015; see Open Technology Fund, "Projects" <<https://www.opentechfund.org/projects/>>; see Tactical Technology Collective, "Security in-a-box" <<https://tacticaltech.org/projects/security-box>> accessed 29 July 2015; see Riseup <<https://help.riseup.net/>> accessed 29 July 2015; see Electronic Frontier Foundation, "Surveillance Self-Defense" <<https://ssd.eff.org/en>> accessed 29 July 2015.

²³⁸ Tim Jordan, *Activism!* 130; see "LOIC" <<http://sourceforge.net/projects/loic/>> accessed on 18 Sept 2014.

²³⁹ See Tim Jordan, *Activism!* 123.

²⁴⁰ Tim Jordan, *Activism!* 123; see also Paul Taylor, "From hackers to hacktivists" 635.

they opt for a quite low-tech approach to disrupting a target's website that simply requires participants to manually and repeatedly press the "reload" button on their web browsers when accessing the site.²⁴⁰ They only wish to slow down the website and not take it completely offline.²⁴¹ Although less efficient, this approach produces similar effects to an automated DoS attack, but is arguably more legally defensible because it requires the genuine and actual involvement of a mass of people, and visiting a website and pressing the reload button is *prima facie* a legitimate and common online activity.²⁴² The benefit and rationale for hacktivists is they "choose a technically inefficient means to serve politically efficient ends".²⁴³

It is important to remember that hacktivists interfere with information systems not for its own sake or as an end in itself, but to promote a political cause or social value that they agree with or believe in.²⁴⁴ More often than not, these social goals and values concern or relate to the "rights of free speech and access to information".²⁴⁵ Hacktivism like traditional activism is ultimately about gaining and raising public awareness, support and engagement for their own or others' socio-political causes and campaigns.²⁴⁶ Their actions are less concerned with damaging or hindering computer data or system *per se*, but are meant to support social movements and promote cultural change. While their activities center on or are directly aimed at technology, their fundamental aim is social action. Hacktivism closely resembles civil disobedience in that they both are "public, non-violent and conscientious act[s] contrary to law... with the intent to bring about a change in the policies or law of the government".²⁴⁷ Hacktiv-

²⁴¹ Tim Jordan, *Activism!* 123.

²⁴² See Tim Jordan, *Activism!* 123.

²⁴³ Tim Jordan, *Activism!* 125.

²⁴⁴ Xiang Li, "Hacktivism and the First Amendment" 304; Argyro Karanasiou, "The changing face of protests in the digital age" 103.

²⁴⁵ Argyro Karanasiou, "The changing face of protests in the digital age" 103.

²⁴⁶ See Tim Jordan, *Activism!* 125; see also Xiang Li, "Hacktivism and the First Amendment" 324-326.

²⁴⁷ Argyro Karanasiou, "The changing face of protests in the digital age" 101 (citing Rawls).

²⁴⁸ Tim Jordan, *Activism!* 125.

ists “aim to enroll people, to draw them into discussion, reflection and action”.²⁴⁸ Enlisting or gaining the support of the general or relevant public is crucial because it does not only improve the chances of success of their campaigns, but, equally important, it provides democratic legitimacy to their actions. As Jordan clarifies,

A mass of people is key, because then the protest is not about one person’s technical abilities, but about the choice of many people to protest. This provides the same legitimation for a protest as thousands of people in the street might. It makes the protest a popular protest.²⁴⁹

As shown above, hacktivism is an exceedingly complex socio-technical phenomenon, and any attempt to label it as an illegal act of data and system interference as opposed to a legitimate form of protest is a difficult exercise. While it is true that “most current forms of hacktivism are rightly regulated or prohibited outright”, there are strong legal and public policy reasons to support the position that “a narrow subset of hacktivism should be protected on the grounds that it is primarily expressive, does not involve the hijacking of computers or networks, and causes no significant damage”.²⁵⁰ Hampson correctly argues that

forms of hacktivism that are primarily expressive, that do not involve obtaining or exploiting illegal access to computers or networks for commercial advantage or financial gain, and that cause little or no permanent damage, should receive at least some protection as a legitimate form of protest.²⁵¹

Thus, a “categorical prohibition on all forms of hacktivism” should be avoided because it “may sweep up socially productive uses of cyberattacks as a form of protest”.²⁵² It must be remembered

²⁴⁹ Tim Jordan, *Activism!* 125.

²⁵⁰ Noah Hampson, “Hacktivism” 542; see also Xiang Li, “Hacktivism and the First Amendment” 304 and 329; see also Argyro Karanasiou, “The changing face of protests in the digital age” 109.

²⁵¹ Noah Hampson, “Hacktivism” 531-532.

²⁵² Xiang Li, “Hacktivism and the First Amendment” 304.

²⁵³ Tim Jordan, *Activism!* 23.

that political protests and social movements manifest and embody changing norms and values within a community or society.²⁵³ Social movements are a prime “source of authoritative ethical visions” and normative expectations of individuals and groups.²⁵⁴ As such, the interpretation and application of the law (including the important concept of “without right”) should be flexible and mutable in order to adjust to people’s changing evaluations and understandings of the appropriate and the desirable, rather than repressing or excising them at the outset. This position is expanded some more in Chapter 6.

4.2.6 MISUSE OF DEVICES

The last species of computer security crime is called misuse of devices. For this offense to apply, the perpetrator must intentionally and without right produce, distribute or make available “a device, including a computer program, designed or adapted primarily for the purpose of committing” other computer security crimes,²⁵⁵ or possess “a computer password, access code, or similar data”, both of which must be carried out with intent to use the device and password to commit such crimes.²⁵⁶ These illicit or prohibited tools include devices, computer programs, computer passwords, access codes and similar data such as stolen credit card numbers and user credentials. Under the Convention, “distribution” requires “the active act of forwarding data to others”, while “making available” involves “placing online devices for the use of others”.²⁵⁷ The rationale for the criminalization of misuse of devices is two-fold. First, authorities want to discourage the acquisition of “hacker tools” for “criminal purposes”.²⁵⁸ This is so be-

²⁵⁴ Tim Jordan, *Activism!* 10.

²⁵⁵ Convention on Cybercrime, art 6 1(a); see also Explanatory Report to the Convention on Cybercrime, para 71; see also Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 10.

²⁵⁶ Convention on Cybercrime, art 6 1(a)ii and 6 1(b); see also Council Directive 2013/40/EU on attacks against information systems, art 7; see also Explanatory Report to the Convention on Cybercrime, paras 71 and 76; see also Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 10.

²⁵⁷ Explanatory Report to the Convention on Cybercrime, para 72.

²⁵⁸ Explanatory Report to the Convention on Cybercrime, para 71.

cause the crime of misuse of devices seems naturally connected to the commission of other computer security crimes discussed above. For instance, the creation or possession of a computer virus is normally a preliminary step to the actual use of the virus to conduct data or system interference.²⁵⁹ Second, criminalizing misuse of devices is meant to serve as a disincentive or deterrence to the creation of a “black market of cybercrime tools”.²⁶⁰ The drafters of the Convention were of the view that “[t]o combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source”.²⁶¹

With respect to its scope of application, the crime of misuse of devices is on the whole carefully circumscribed. As explained by the drafters of the Convention,

In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counterattacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent that the device is used for the purpose of committing any of the offences established in Articles 25 of the Convention.²⁶²

This means that for the offense of misuse of devices to be committed, the general intent to make available or possess the illicit tool or access code must be coupled with a specific or direct intent that such tool or code is to be used for the purpose of breaching the security of a computer system or data. The Convention explicitly states that there should be no criminal liability if the tool or code “is not for the purpose of committing” a computer security crime “such as for the authorised testing or protection of a computer system”.²⁶³ As further explained by the Convention drafters,

²⁵⁹ Explanatory Report to the Convention on Cybercrime, para 72.

²⁶⁰ Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 10; see also Explanatory Report to the Convention on Cybercrime, para 71.

²⁶¹ Explanatory Report to the Convention on Cybercrime, para 71.

²⁶² Explanatory Report to the Convention on Cybercrime, para 76.

²⁶³ Convention on Cybercrime, art 6 2.

tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression “without right”. For example, testdevices (“crackingdevices”) and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be “with right”.²⁶⁴

The offense of misuse of devices is therefore restricted “to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone usually excludes dualuse devices”.²⁶⁵ This policy position is adopted as well in the Cybercrime Directive.²⁶⁶

The crime of misuse of devices does not appear to be too troublesome for makers and hacktivists.²⁶⁷ The hacking tools, information and instructions that they produce, distribute, make available or possess do not fall within the purview of misuse of devices because they are more often than not publicly released or explicitly marketed for legitimate purposes such as security testing, privacy enhancement, reverse engineering, interoperability, technical improvements, replacement or repair, academic research, education and public awareness, and for other public interests.²⁶⁸ Even LOIC, a popular tool among hacktivists to perform DoS attacks, is promoted as dual-use technology that is a “network stress testing and denial-of-service attack application”.²⁶⁹ While there is nothing in the law that can prevent an overzealous or overreaching public prosecutor from filing a case, the law

²⁶⁴ Explanatory Report to the Convention on Cybercrime, para 77.

²⁶⁵ Explanatory Report to the Convention on Cybercrime, para 73; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 10.

²⁶⁶ Council Directive 2013/40/EU on attacks against information systems, recital 16.

²⁶⁷ See Explanatory Report to the Convention on Cybercrime, para 73; but see Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on attacks against Computer Systems” 10; .

²⁶⁸ See Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 8.

²⁶⁹ LOIC, <<http://sourceforge.net/projects/loic/>> accessed on 3 October 2014; see also Argyro Karanasiou, “The changing face of protests in the digital age” 102.

²⁷⁰ See Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 9.

is quite clear that unless there is also a specific intent that the devices and codes are to be used to commit criminal acts then no liability should attach to their mere production, possession or distribution.²⁷⁰ Makers and hackers can thus avoid prosecution through the simple expedient of expressly highlighting or publicly making known the fact that their devices, programs and codes are primarily intended for legitimate purposes. Of course, any claim of legitimate purpose and use will only stand if the producers, distributors, users and possessors of these tools and codes do not perform acts or engage in other activities that belie their asserted benign purposes.

4.3 Intellectual property laws

4.3.1 FRAUGHT HISTORY OF INTELLECTUAL PROPERTY AND SOCIO-TECHNICAL INNOVATION

While their effects on hacking may not be as direct, immediate and pronounced as those associated with computer crime laws, intellectual property laws similarly have a deep and far-reaching impact on the freedom and ability of makers and hackers to engage in their personal and social projects and pursuits. The uneasy relationship between hacking and intellectual property is quite understandable given that technological innovations in general have an intimate yet conflict-ridden history with intellectual property laws.²⁷¹ The first intellectual property law, the Statute of Anne (a copyright legislation enacted in 1710),²⁷² was a reaction to the invention, widespread use and disruptive changes brought about by the movable-type printing press.²⁷³ Since then, additions, modifications, revisions and expansions to intellectual property laws have occurred virtually in lockstep with the

²⁷¹ See Jane Ginsburg, "Copyright and Control Over New Technologies of Dissemination" 1617, 1619 and 1620; see Michael Dizon, "Does Technology Trump Intellectual Property?" 125.

²⁷² Jessica Litman, *Digital Copyright* 15.

²⁷³ Lawrence Lessig, *Code*: version 2.0 172; Nicola Lucchi, "The supremacy of techno-governance" 200; see also James Boyle, *The Public Domain* 8.

²⁷⁴ Lawrence Lessig, *Code*: version 2.0 172.

emergence and adoption of techno-social advances and changes.²⁷⁴ For instance, the major treaty revisions to the Berne Convention were done “to find responses to new technological developments (such as sound recording technology, photography, radio, cinematography and television).”²⁷⁵ As Lessig recounts, the invention of sound recording machines resulted in the creation of new recording rights at the turn of the 20th century, the advent of radio produced performance rights, and the popularity of cable television led to the statutory grant of rebroadcast rights.²⁷⁶ But the relations between technology and intellectual property are far from being one-way or asymmetric. As was evident with the first generations of hackers, the assertion, exploitation and enforcement of intellectual property rights can both adversely and positively affect the practices and culture of a technical and epistemic community, as well as the production and dissemination of technology as a whole. The propensity of intellectual property and technological innovations to be at odds with each other has much to do with the goals, norms and values sought and embedded in intellectual property laws, and the delicate balancing of multiple, complex and competing interests that are at the heart of the laws and policies on technology, information and innovation.²⁷⁷ These clashes between technical innovation and intellectual property are quite evident in the case of makers and hacktivists where the norms and value of hacking often come into conflict with the aims of intellectual property laws.

4.3.2 INTELLECTUAL PROPERTY BALANCE

The term “intellectual property” broadly refers to “the legal rights which result from intellectual activity in the industrial, scientific-

²⁷⁵ WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2; see also Michael Dizon, “Does Technology Trump Intellectual Property?” 130-131.

²⁷⁶ Lawrence Lessig, Code: version 2.0 172; see also Jessica Litman, Digital Copyright 18; see also Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1616 and 1627.

²⁷⁷ See Lawrence Lessig, Code: version 2.0 192.

²⁷⁸ WIPO, WIPO Intellectual Property Handbook 3; see also Berne Convention for the Protection of Literary and Artistic Works, art 2(1).

ic, literary and artistic fields”.²⁷⁸ There are many kinds of intellectual property rights and they apply to various forms of intellectual creations or “creations of the mind”.²⁷⁹ Basically, copyright covers “literary and artistic works” or expressions of ideas (such as computer code and programs, printed manuals, written instructions, and technical drawings, plans and specifications);²⁸⁰ patents²⁸¹ are granted for novel and non-obvious inventions that are capable of industrial application (e.g., 3D printing technologies, computer hardware, and certain computer-implemented inventions with a “further technical effect”);²⁸² trademarks are distinctive signs used to identify goods and services (e.g., marks or logos of FOSS projects like Linux, Firefox and Android);²⁸³ industrial designs “protect the original ornamental and non-functional features of an industrial article or product that result from design activity” (like the design of and ornamentations on devices);²⁸⁴ databases are granted sui generis protection in Europe in light of the “investment of considerable human, technical and financial resources” for their arrangement, storage and access (i.e., information and data stored on computer systems and servers);²⁸⁵ and the sui generis protection of topographies of integrated circuits covers the layout-designs of electronic circuits and semiconductor chips (which are an integral part of those all-important microprocessors, memory chips, microcontrollers and printed circuit boards that lie at the heart of computer systems and

²⁷⁹ WIPO, WIPO Intellectual Property Handbook 422; see Agreement on Trade-Related Aspects of Intellectual Property Rights, art 1(2) and (3).

²⁸⁰ Berne Convention for the Protection of Literary and Artistic Works, art 2(1); see also Agreement on Trade-Related Aspects of Intellectual Property Rights, art 9(2) and 10; see also Dutch Copyright Act, arts 1 and 10; see also Case C-406/10 SAS Institute Inc. v World Programming Ltd [2012], paras 32 and 46.

²⁸¹ Paris Convention for the Protection of Industrial Property; Agreement on Trade-Related Aspects of Intellectual Property Rights, art 27 (1); see also WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 2 and 19.

²⁸² See Convention on the Grant of European Patents (European Patent Convention); see European Patent Office, “Patents for software? European law and practice” 13-14; see Andres Guadamuz, “The Software Patent Debate”; see Robin Widdison, “Software Patents Pending?”.

²⁸³ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 15.

²⁸⁴ WIPO, WIPO Intellectual Property Handbook 112; see also Agreement on Trade-Related Aspects of Intellectual Property Rights, art 25(1).

²⁸⁵ Directive 96/9/EC on the legal protection of databases, recitals 7 and 13.

²⁸⁶ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 35 and 36; see also Treaty on Intellectual Property in Respect of Integrated Circuits.

information technologies).²⁸⁶

Despite the various types of intellectual property, it may be said that intellectual property laws are ultimately about balancing the rights of control and access to creative information, knowledge and know-how,²⁸⁷ which is why it is extremely relevant to hacking. The main purposes and rationale of intellectual property laws are two-fold:

One is to give statutory expression to the moral and economic rights of creators in their creations and the rights of the public in access to those creations. The second is to promote, as a deliberate act of Government policy, creativity and the dissemination and application of its results and to encourage fair trading which would contribute to economic and social development.²⁸⁸

Intellectual property rights are legislative creations, i.e. statutorily granted limited monopolies on specific uses of intangible property.²⁸⁹ According to Lessig, “Intellectual property rights are a monopoly that the state gives to producers of intellectual property in exchange for their production of it. After a limited time, the product of their work becomes the public’s to use as it wants”.²⁹⁰ There is strong support for intellectual property rights from a legal and public policy perspective because they are believed to play a key role in “economic, social and cultural growth”.²⁹¹ Intellectual property laws are geared towards the incentivization, promotion and protection of cultural and technical creativity, invention and innovation for the benefit of both creators and society as a whole.²⁹² There is, thus, inextricably bound in the kernel of intellectual property

²⁸⁷ Hector MacQueen and others, *Contemporary Intellectual Property* 7; Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 559.

²⁸⁸ WIPO, *WIPO Intellectual Property Handbook* 3.

²⁸⁹ See James Boyle, *The Public Domain* 11; Lawrence Lessig, *Code: version 2.0* 185.

²⁹⁰ Lawrence Lessig, *Code: version 2.0* 184; see also James Boyle, *The Public Domain* 4.

²⁹¹ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 7.

²⁹² Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1613; James Boyle, *The Public Domain* 1.

laws and policies, a legal and social imperative to strike a balance between the grant of exclusive rights to creators and the right of the public to gain access to and use such intellectual creations.²⁹³ This so-called “intellectual property balance” is an integral part of intellectual property laws and rights. As stated in Article 7 of the TRIPS Agreement:

The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.²⁹⁴

Intellectual property laws are ultimately meant to “to achieve the optimal balance between the grant of incentives to create and the right of the public to use such creations”.²⁹⁵ As Lessig explains,

The balance that intellectual property law traditionally strikes is between the protections granted the author and the public use or access granted everyone else. The aim is to give the author sufficient incentive to produce. Built into the law of intellectual property are limits on the power of the author to control use of the ideas she has created.²⁹⁶

The ability of persons and the wider public to access and make use of others’ intellectual creations is thus an indispensable component and consideration of the intellectual property balance.

It should be pointed out, though, that it is the “law [that] strikes this balance. It is not a balance that would exist in nature”.²⁹⁷ As

²⁹³ Niva Elkin-Koren, “Copyright policy and the limits of freedom of contract” 97 and 100; Pamela Samuelson “Challenges for the World Intellectual Property Organisation and the Trade-Related aspects of Intellectual Property Rights Council in regulating intellectual property rights in the information age” 539 and 541; see WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 3 and 19.

²⁹⁴ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 7.

²⁹⁵ Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 565; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 39.

²⁹⁶ Lawrence Lessig, Code: version 2.0 184; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 31.

²⁹⁷ Lawrence Lessig, Code: version 2.0 185.

affirmed by the WIPO Standing Committee on Copyright and Related Rights, “[s]triking this balance is left as a matter for national legislation. Value judgments will need to be made, and these will clearly vary according to the society and culture concerned”.²⁹⁸ While it is true that the law and public authorities traditionally bear the onus of “balancing incentives to create and accessibility of information”,²⁹⁹ it is important not to downplay the vital role that public and socio-cultural practices play in locating and adjusting this balance. Determining, establishing and preserving such a delicate or optimal equilibrium between the competing requirements of incentives/control vis-à-vis access and use is critical because it must “reflect the balance between the need to induce creation and the need to guarantee public access to information”, as well as the ability of members of the public to reasonably use such works and inventions.³⁰⁰

In actuality, however, achieving the right balance between control versus access (whether through legislative enactments, policy directives, enforcement actions or everyday practices) is neither straightforward nor unproblematic.³⁰¹ In fact, together with the growth and popularity of computing, digital technologies and information networks since the 1970s, there has been an ineluctable march towards an ever-increasing expansion, protection and strict enforcement of intellectual property rights at the expense of the public’s right to access and use information and technology.³⁰² These changes in intellectual property laws were precipitated by “new technological developments” such as, among others, “reprography, videotechnology, compact cassette systems facilitating ‘home taping,’ satellite broadcasting, cable

²⁹⁸ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 26.

²⁹⁹ Niva Elkin-Koren, “Copyright policy and the limits of freedom of contract” 100; Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1613.

³⁰⁰ Niva Elkin-Koren, “Copyright policy and the limits of freedom of contract” 100, 102 and 109; see also Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” __; Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 25 and 26.

³⁰¹ Lawrence Lessig, Code: version 2.0 185.

³⁰² James Boyle, The Public Domain 46, 49 and 50; see also Peter Drahos and John Braithwaite, Information Feudalism 4-5;

³⁰³ WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2; see also Michael Dizon, “Does Technology Trump Intellectual Property?” 129-130.

television, the increase of the importance of computer programs, computer-generated works and electronic databases”.³⁰³ The succeeding decades saw the formal and express acknowledgement of copyright protection over software,³⁰⁴ as well as the legal recognition of patents over software (in the United States) and computer-implemented inventions (in Europe and other parts of the world).³⁰⁵ The expansion and ratcheting up of intellectual property rights continued through the 1990s and early 2000s on both an international and national level with the adoption of the TRIPS Agreement, the WIPO Internet Treaties, bilateral agreements and national anti-circumvention laws,³⁰⁶ the recognition of the applicability and enforceability of copyright in the digital environment,³⁰⁷ and the corresponding case law and jurisprudence based on these treaties and statutes. Whether individually or in aggregate, these laws and policies on intellectual property have had a long-standing impact on the production and dissemination of innovation and other techno-social practices (including hacking).

³⁰⁴ See Pamela Samuelson, “Freedom to Tinker” 10; see also Agreement on Trade-Related Aspects of Intellectual Property Rights, art 10(1).

³⁰⁵ *Diamond v. Diehr* 450 U.S. 175 (1981); WIPO Copyright Treaty, art 4; Directive 2009/24/EC on the legal protection of computer programs, art 1; European Patent Office, “Patents for software? European law and practice” <<http://www.epo.org/news-issues/issues/software.html>> accessed 24 July 2015; see also Robin Widdison, “Software Patents Pending?”.

³⁰⁶ See Agreement on Trade-Related Aspects of Intellectual Property Rights; see WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (known as the WIPO Internet Treaties); Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society; see Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 2; see WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 3; see WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 5; see WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 51.

³⁰⁷ WIPO Copyright Treaty WCT, art 1(4); Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society; WIPO, Agreed Statements concerning the WIPO Copyright Treaty, see also WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 56, 78 and 79; see also WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 5; see also WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 3.

4.3.3 BROAD EXCLUSIVE RIGHTS YET NARROW LIMITATIONS AND EXCEPTIONS

Quite a number of legal and scholarly writings have been published decrying the current state of affairs of intellectual property rights.³⁰⁸ These scholars believe that, with regard to the intellectual property balance, “the pendulum has swung too far” in favor of incentivizing creators to the detriment of public access to and use of intellectual creations.³⁰⁹ Under the current legal regime of intellectual property, the exclusive rights granted to creators are expansive and interpreted broadly, whereas the limitations and exceptions to these rights are very specific and narrowly applied.³¹⁰

Of the many kinds of intellectual property rights, copyright and patents are the most material to makers and hacktivists. Copyright consists of a bundle of exclusive rights to authorize the reproduction, translation, adaptation, alteration, making derivatives, distribution, public performance, communication to the public, making available to the public, rent and use of literary and artistic works.³¹¹ Patents grant inventors or owners the exclusive rights to prevent third parties from “making, using, offering for sale, selling, or importing” the patented

³⁰⁸ See James Boyle, *The Public Domain*; see Peter Drahos and John Braithwaite, *Information Feudalism*; Lawrence Lessig, *Free Culture*; see Lawrence Lessig, *The Future of Ideas*; see Jessica Litman, *Digital Copyright*; see Hal Abelson, Ken Ledeen and Harry Lewis, *Blown to Bits*; see Keith Aoki, James Boyle and Jennifer Jenkins, *Bound by Law*; see Kathy Bowrey, *Law and Internet Cultures*; see James Boyle, *Shamans, Software, and Spleens*.

³⁰⁹ Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1614; see also James Boyle, “A manifesto on WIPO and the future of intellectual property” (2004) *Duke Law & Technology Review* No. 9, 2; Peter Drahos, “Bilateralism in Intellectual Property” *Oxfam GB*, 9; see also Declan McCullagh and Milana Homsi, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 328.

³¹⁰ Jessica Litman, *Digital Copyright* 18, 54 and 78; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 29 and 31; see also P. Bernt Hugenholtz and Ruth Okediji, “Conceiving an International Instrument on Limitations and Exceptions to Copyright” 22, 23, 28; see also Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 4.

³¹¹ *Berne Convention for the Protection of Literary and Artistic Works*, arts 8, 9, 11, 11bis, 11ter, 12 and 14; *Agreement on Trade-Related Aspects of Intellectual Property Rights*, art 11; *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*, arts 2, 3 and 4; see *Dutch Copyright Act*, arts 12 and 13.

³¹² *Agreement on Trade-Related Aspects of Intellectual Property Rights*, art 28(1)(a) and art 28(2); see also WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 18.

³¹³ *Agreement on Trade-Related Aspects of Intellectual Property Rights*, art 28(1)(b).

products without their consent.³¹² With regard to patented processes, inventors have exclusive rights to stop other persons and entities from “using the process”,³¹³ as well as to bar the use, offer for sale, sale, or import of products “obtained directly by that process”. These exclusive rights on their face seem to be relatively fair and reasonable. However, due to the confluence of socio-technical trends such as the growing digitization of information and the centrality of technology in the networked society, coupled with the ever-expanding and deepening scope of intellectual property rights, the impact and applicability of copyright and patents on hacking and technology development as a whole have never been as great or as far reaching as it currently exists, and will continue to be so.³¹⁴ The intensifying digitization and technologization of social life means many aspects of people’s behaviors and activities whether online and offline are subject to intellectual property laws and rights.³¹⁵ Lessig remarks that “in the digital world, life is subject to copyright law. Every single act triggers the law of copyright. Every single access or use is either subject to a license or illegal, unless” it is subject to a statutory limitation or exception such as the right to make quotations.³¹⁶ As many aspects of people’s lives are mediated by and through various computing and information technologies,³¹⁷ copyright and patent laws and rights pervade and influence people’s actions and what they are able to do with their own and others’ information and technologies.³¹⁸ This also means that, “[b]ecause of the changes in digital technology, it is now possible for the law to regulate every single use of creative work in a digital environment”.³¹⁹

Despite the current state of affairs, it should be remembered that limitations and exceptions to intellectual property rights were cen-

³¹⁴ See Lawrence Lessig, Code: version 2.0 192-193; Urs Gasser and Silke Ernst, “A Quick Look at Copyright and User Creativity in the Digital Age” 3, 11 and 13.

³¹⁵ See Lawrence Lessig, Code: version 2.0 192-193.

³¹⁶ Lawrence Lessig, Code: version 2.0 193.

³¹⁷ See Llewellyn Joseph Gibbons, “Social Enforcement or Social Contracting for Governance in Cyberspace” 485; see Michael Dizon, “Participatory democracy and information and communications technology” 1.

³¹⁸ Lawrence Lessig, Free Culture 184, 185, 188, 192; see also Keith Aoki, James Boyle and Jennifer Jenkins, Bound by Law.

³¹⁹ Lawrence Lessig, Code: version 2.0 196.

tral policy issues and areas of debate even during the negotiations of the Berne Convention in the 1880s and other subsequent international treaties because of their essential role in maintaining the intellectual property balance.³²⁰ As explained by WIPO Standing Committee on Copyright and Related Rights, “[i]t has long been recognized that restrictions or limitations upon authors, and related rights may be justified in particular cases” and “limits to absolute protection are rightly set by the public interest”.³²¹ For instance, limitations and exceptions to copyright have been justified based on the following purposes and grounds: informatory, educational, public access, convenience, archival preservation, new industry, state power, *de minimis*, necessity, and public interest.³²² It should be noted that these and other limitations and exceptions to intellectual property rights are based on economic as well as “non-economic ‘public policy’ considerations”.³²³ While intellectual property laws *prima facie* seem to place greater emphasis on creators and their exclusive economic and moral rights, it bears stressing that these laws are also “underpinned by some kind of non-author centered and non-economic normative consideration” whether it be freedom of information, participatory democracy, public debate and discourse, education, or information and knowledge distribution.³²⁴

As things currently stand, the restrictive application and uses of intellectual property laws tend to restrain the ability of makers and hacktivists to engage in the common acts of hacking – to explore, break, learn, create, share and secure information and technologies. Furthermore, the statutory limitations and exceptions are narrowly

³²⁰ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 5-6.

³²¹ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 3 and 75.

³²² Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 42, 43 and 75; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 8-9.

³²³ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 25.

³²⁴ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 25; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 20.

³²⁵ See Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 3, 4, 10, 42 and 43.

circumscribed and only some of them are relevant or directly apply to hacking.³²⁵ Notwithstanding the legal obstacles and constraints that are firmly in place, the few limitations and exceptions to intellectual property rights do provide some albeit limited space and freedom for makers and hackers to carry out their hacking projects and campaigns.³²⁶ Quite interestingly though, despite or perhaps because of these restrictions, hackers tend to reside and even thrive in the gaps, contradictions and margins of the law (see Sections 5.2.2 and 5.2.3).

The following limitations and exceptions under international, European and Dutch copyright and patent laws afford makers and hackers (as well as ordinary users) some agency and play to creatively and constructively access and use information and technology.

4.3.3.1 Reverse engineering, decompilation and use of software

Directive 2009/24/EC on the legal protection of computer programs (the Software Directive) contains two exceptions to the exclusive rights of copyright that are indispensable to hacking – reverse engineering and decompiling of software.³²⁷ Reverse engineering is a highly technical process whereby “a person other than the original program developer is able to determine the ideas and principles that underlie the functional elements of the software by examining its external inputs and outputs”.³²⁸ Also called “black box” analysis, this form of reverse engineering does not require direct access to the computer program’s source code and other hidden or internal specifica-

³²⁶ See Pamela Samuelson, “Freedom to Tinker” 3.

³²⁷ Directive 2009/24/EC on the legal protection of computer programs, arts 1(1), 5 and 6 and recital (6); see also Council Directive of 1 May 1991 on the legal protection of computer programs (which Directive 2009/24/EC amended and codified); see also Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 213.

³²⁸ Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214; see also Thomas Vinje, “Compliance with Article 85 in software licensing” 171; see also Erik Kroker, “The Computer Directive and the balance of rights” 248; see also Case C-406/10 SAS Institute Inc. v World Programming Ltd [2012], paras 32, 40 and 46.

³²⁹ John Soma, Gus Winfield and Letty Friesen, “Software Interoperability and Reverse Engineering” 195; Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214.

tions.³²⁹ The Software Directive expressly provides that a person “shall be entitled, without the authorization of the right-holder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program”.³³⁰ The ability to reverse engineer though is subject to the conditions that such person has “a right to use a copy of a computer program” and it must be done “while performing any of the acts of loading, displaying, running, and transmitting or storing the program which he is entitled to do so”.³³¹ Unlike decompilation, reverse engineering does not have to be limited to achieving interoperability and can be undertaken for such bread-and-butter hacker activities as observing, studying or testing how a program works.³³²

Decompilation, for its part, entails accessing and studying the actual code and internal workings of the computer program.³³³ It should be noted that decompilation is more strictly regulated compared to black box analysis since the former can only be undertaken when it is “indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs”.³³⁴ Furthermore, it is subject to a number of conditions: first, the decompilation must be “performed by the licensee or by another person having a right to use a copy of a program”; second, “the information necessary to achieve interoperability has not previously been readily available to the person”; and, third, it is “confined to the parts of the original program which are necessary in order to achieve interoperability”.³³⁵ There are also additional cave-

³³⁰ Directive 2009/24/EC on the legal protection of computer programs, art 5(3); see also Dutch Copyright Act, art 45l; see also Case C-406/10 SAS Institute Inc. v World Programming Ltd [2012], para 62; see also WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 48.

³³¹ Directive 2009/24/EC on the legal protection of computer programs, art 5(3); see also Krause v Titleserv, Inc., 402 F.3d 119 (2005) (for US perspective); see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 23.

³³² Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214; see Erik Kroker, “The Computer Directive and the balance of rights” 248.

³³³ Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214; see also Thomas Vinje, “Compliance with Article 85 in software licensing” 172.

³³⁴ Directive 2009/24/EC on the legal protection of computer programs, art 6(1); see also Dutch Copyright Act, art 45m(1).

³³⁵ Directive 2009/24/EC on the legal protection of computer programs, art 6(1)(a), (b) and (c); see also Dutch Copyright Act, art 45m(1)(a-c); Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214.

ats on what a person can do with the information obtained through decompilation. Such decompiled data can only be used to “achieve interoperability” with an “independently created program”, it cannot “be given to others, except when necessary for the interoperability of the independently created computer program”, and it must not “be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright”.³³⁶ If these restrictions were not enough, the Software Directive also has a general “safeguard clause”, which states that the decompilation provisions should be narrowly interpreted and must not be applied “in a manner which unreasonably prejudices the rightholder’s legitimate interests or conflicts with a normal exploitation of the computer program”.³³⁸ In any event, as with reverse engineering, the right to decompile software cannot be waived, bargained away or contravened by contract and any stipulations to the contrary are null and void. The Court of Justice of the European Union explained the rationale for the law’s prohibition against such contractual stipulations in the landmark case of *SAS Institute v World Programming*: “Article 5(3) of Directive 91/250 seeks to ensure that the ideas and principles which underlie any element of a computer program are not protected by the owner of the copyright by means of a licensing agreement”.³³⁹ In the United States though, there have been conflicting court decisions on the validity or enforceability of license clauses that prevent the licensee or user from reverse engineering or decompiling a computer program because there is no express statutory prohibition under US law.³⁴⁰

³³⁶ Directive 2009/24/EC on the legal protection of computer programs, art 6(2)(a), (b) and (c); see also Dutch Copyright Act, art 45m(2)(a-c).

³³⁷ Directive 2009/24/EC on the legal protection of computer programs, art 6(3); see also Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214.

³³⁸ Directive 2009/24/EC on the legal protection of computer programs, art 8 and recital (16); Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 218.

³³⁹ Case C-406/10 *SAS Institute Inc. v World Programming Ltd* [2012], paras 51, 53 and 59.

³⁴⁰ See Pamela Samuelson, “Freedom to Tinker” 14.

Interestingly, in addition to reverse engineering and decompilation, the Software Directive recognizes a limited but valuable exception to the exclusive rights granted to the original software developer – the right to use. Under the law, users who lawfully acquired a program have a general and quite obvious right to use it, and such use “shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction”.³⁴¹ A US court has similarly ruled that “[c]onsumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software. What the law authorizes, [the company] cannot revoke”.³⁴² While this general right to use may be modified or suppressed through contractual stipulations, there are specific rights of use such as “making a back-up copy” and the “act of correction of its errors” cannot be prohibited or avoided by contract.³⁴³

It is quite apparent that the drafters of the Software Directive sought to balance the exclusive rights of the original program developers with the right of users to make reasonable and even innovative (in case of reverse engineering or decompilation) uses of computer programs.³⁴⁴ While it is possible to argue whether they did not go far enough or they went too far,³⁴⁵ the drafters seem to be well aware of a fundamental and incontrovertible principle about software and technology as a whole – they are meant to be used. As stated in Software Directive, “The function of a computer program is to communicate and work together with other components of a computer system and

³⁴¹ Directive 2009/24/EC on the legal protection of computer programs, art 5(1) and recital (14); see also Dutch Copyright Act, art 45j; see also Case C-406/10 SAS Institute Inc. v World Programming Ltd [2012], paras 56 and 58.

³⁴² Chamberlain Group v Skylink Technologies 381 F. 3d 1178 (2004), 1202.

³⁴³ Directive 2009/24/EC on the legal protection of computer programs, art 5(1) and (2) and recitals 13 and 16; see also Dutch Copyright Act, arts 45j and 45k.

³⁴⁴ See Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214; see Robert Hart, “Interoperability information and the Microsoft decision” 116.

³⁴⁵ See Robert Hart, “Interfaces, interoperability and maintenance” 111; see Thomas Vinje, “Compliance with Article 85 in software licensing” 165; see Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214.

³⁴⁶ Directive 2009/24/EC on the legal protection of computer programs, recital 10.

³⁴⁷ See Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 215-216 (for more on interoperability).

with users”.³⁴⁶ While this statement primarily concerns the value of interoperability in and of computer systems and data,³⁴⁷ it likewise speaks to the desirability of ensuring, as a matter of public policy, that people (including hackers) are able to actually use software and understand how it works.³⁴⁸ The rights to reverse engineering, decompile and use software are indeed pertinent to makers and other types of hackers because they directly involve the common acts of hacking (explore, break, learn and create), and the information or knowledge gained from these activities may be utilized to perform or pursue other common acts (share and secure). In addition, reverse engineering and decompilation are clearly connected to and may be used to advance the hacker norms and values of openness, freedom of access, transparency and curiosity.

4.3.3.2 Temporary acts of reproduction

Closely related to the above exceptions for reverse engineering, decompilation and use of software is the limitation for temporary acts of reproduction.³⁴⁹ Under Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (the Copyright Directive) and its implementation into Dutch law, temporary acts of reproduction that “are transient or incidental [and] an integral and essential part of a technological process” do not require the authorization of the copyright owner.³⁵⁰ This exemption is subject to the condition that the “sole purpose” of the reproduction is “to enable” a “lawful use” or “a transmission in a network between third parties by an intermediary”.³⁵¹ Furthermore,

³⁴⁸ See Michael Dizon, “Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy” 214.

³⁴⁹ See Report on application of Directive 2001/29/EC SEC(2007) 1554, 4; see WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 14.

³⁵⁰ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(1); Dutch Copyright Act, art 13a.

³⁵¹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(1)(a-b).

³⁵² Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(1); Dutch Copyright Act, art 13a.

³⁵³ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 33.

such temporary reproduction should have “no independent economic significance”.³⁵² A use is deemed lawful “where it is authorised by the rightholder or not restricted by law”.³⁵³

According to the drafters of the Copyright Directive, the policy rationale for this limitation is due to the fact that

its transient and incidental character may point to the lack of any real economic conflict with the normal exploitation of protected works, while the fact that it is an integral and necessary part of a larger process leading to a communication of a work may indicate that this is not something that the author/right-holder needs to control.³⁵⁴

Examples of normal or everyday uses of information technologies that produce such exempted temporary copies include “reproductions on Internet routers, reproductions created during web browsing or copies created in Random Access Memory (RAM) of a computer, copies stored on local caches of computer systems or copies created in proxy servers”.³⁵⁵ This limitation on the reproduction right is sensible given that, in order to properly access and use any software or digital content, it is necessary for parts or the entire work to be reproduced as part of the normal functions and operations of a computer or information system.³⁵⁶ The exemption for temporary acts of reproduction is clearly analogous to the right to use of software under the Software Directive although the former applies more broadly to any copyrighted work, especially those in digital form. And like the right to use software, the exception for making transient and incidental copies ensures that makers and hacktivists can safely engage in some com-

³⁵⁴ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 79-80.

³⁵⁵ European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 3; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 33; see also Bradley J. Nicholson, “The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc., and the Problem of Copying in RAM”.

³⁵⁶ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 33; WIPO “Exception and Limits to Copyright and Neighboring Rights” 32 (“logic of a ‘necessary act’”); see Bradley J. Nicholson, “The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc., and the Problem of Copying in RAM”; see Pamela Samuelson, “Hacking Intellectual Property Law” 66 and 67; see WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 80.

mon acts of hacking, especially explore, learn and create.

4.3.3.3 Private and non-commercial copying and use

Copyright and patent laws contain an important exception for private and non-commercial uses of protected works. While it is true that “private copying is not a right but a statutory exception” and it is not found in the Berne Convention,³⁵⁷ “[t]he principle of freedom to make private copies appears in almost all regimes, but in very different forms or stated in very different ways”.³⁵⁸ The Copyright Directive provides for a private copying exception whereby “reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial” do not require the right holder’s authorization.³⁵⁹ Similarly, under the Dutch Copyright Act, a copy or reproduction that is “carried out without any direct or indirect commercial motivation and is intended exclusively for personal exercise, study or use by the natural person who made the reproduction” is an excepted use.³⁶⁰ According to a WIPO study, “private” should be understood as being “distinct from ‘professional’ or ‘commercial’ uses”.³⁶¹ It should be noted that only individual persons can avail of the private use exception and such use or copying must be done for non-commercial purposes. “Non-commercial” has been interpreted as meaning “such uses do not conflict with the normal exploitation of the work... and that this is a non-economic normative factor that is to be weighed against the author’s economic interests”.³⁶² This exception of course is subject to the requirements that “rightholders receive fair

³⁵⁷ European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 4; see also WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 42-43.

³⁵⁸ WIPO “Exception and Limits to Copyright and Neighboring Rights” 12; see also WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 10.

³⁵⁹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(2)(b); see also WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 74.

³⁶⁰ Dutch Copyright Act, art 16c(1); see also Dutch Copyright Act, art 16b(1); see also Martin Senftleben, “The Emerging EC Fair Use Doctrine” 531.

³⁶¹ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 44.

³⁶² WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 75.

compensation”, the procedure for which is provided for under national law.³⁶³ It should be noted as well that the private copying exception does not apply to software under the Dutch Copyright Act and the Software Directive.³⁶⁴

Patent laws contain a similar exception to the exclusive rights of patent holders for private and non-commercial uses and purposes.³⁶⁵ According to a WIPO study, “[i]t is common not to extend the exclusive patent rights to third parties’ activities that are performed in the private sphere or for non-commercial purposes only”.³⁶⁶ As long as a patented product or process is used for personal and non-commercial purposes, then it is covered by an explicit exception under most jurisdictions.³⁶⁷ The Dutch Patent Act contains a similar exception for non-business uses.³⁶⁸

The private use and copying exception benefits makers and hacktivists. This means that they have some freedom to hack, access and use any copyrighted works or patented technologies that they lawfully possess as long as they do so in private and for personal, non-commercial uses, which most hackers are inclined to do anyway at the outset. Pursuant to this exception, makers and hacktivists have the ability to explore, break, learn, create and secure information and technologies. The one major caveat though is that because the exception is limited to private and non-commercial uses, makers and hacktivists cannot distribute or share their innovations with others, especially the wider public, without potentially running afoul of the exclusive

³⁶³ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(2)(b); see also WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 74.

³⁶⁴ Dutch Copyright Act, art 45n; Directive 2009/24/EC on the legal protection of computer programs, arts 4-6; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 50.

³⁶⁵ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 26.

³⁶⁶ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 26.

³⁶⁷ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 26.

³⁶⁸ Dutch Patent Act, art 53(1)(a) and (b); see also WIPO Standing Committee on the Law of Patents, “Report on the International Patent System” SCP/12/3 Rev.2, Revised Annex II.

rights of copyright or patent holders. This prohibition on sharing is at odds with hacker norms and values of openness, freedom of access, freedom of information, community development, and social development.

4.3.3.4 Scientific research and teaching

Another important exception to copyright and patents laws is the ability to copy or use intellectual creations for purposes of teaching or scientific research. Under the Copyright Directive, the authorization of the copyright holder is not required in cases of “use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author’s name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved”.³⁶⁹ The act of teaching covers “elementary as well as advanced teaching and works intended for self- instruction”.³⁷⁰ The drafters of the Copyright Directive elucidate the scope and limitations of this exception in relation to educational institutions:

When applying the exception or limitation for non-commercial educational and scientific research purposes, including distance learning, the non-commercial nature of the activity in question should be determined by that activity as such. The organisational structure and the means of funding of the establishment concerned are not the decisive factors in this respect.³⁷¹

The exception thus also covers any copying or use of protected works done by for-profit education institutions as long as it is undertaken for education or scientific research purposes.³⁷² This exception may be useful for hackers or security researchers who work in or in association with universities or other educational institutions.

³⁶⁹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(3)(a); Dutch Copyright Act, art 16.

³⁷⁰ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 32.

³⁷¹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 42.

³⁷² But see Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 32.

While copyright laws generally require that the copying and use exception for teaching purposes must be done as part of or within the confines of formal education, the exception for scientific research is much broader. It can be done outside of an educational setting, it applies to any person undertaking what is broadly understood as scientific research and not just scientists, and it is done in private.³⁷³ Like the teaching exception, it is the nature and purpose of the activity (i.e., non-commercial and for scientific purposes) that determines the applicability of the exception for scientific research. Since many hacking projects and activities have as their initial goals to explore and learn how things work (which may be deemed scientific pursuits), makers, hacktivists and other hackers can claim protection under the research exception.

Patent laws also have a similar exception for scientific research and experimental purposes.³⁷⁴ Under Dutch law, there is an exception for acts done solely for research on the patented invention.³⁷⁵ The exemption for scientific research and experiments “enables researchers to examine the stated effects of patented inventions and improve such patented inventions without having to fear infringing the patent”.³⁷⁶ As explained by the WIPO Standing Committee on the Law of Patents, the policy rationale for this exception is the importance of creating a “positive environment for research activities” that can “add to the development of technologies, which is precisely one of the objectives of the patent system”.³⁷⁷ The WTO Dispute Settlement Panel similarly confirmed in the *Canada - Patent Protection of Pharmaceutical Prod-*

³⁷³ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 15 and 45; Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 42; Hector MacQueen and others, *Contemporary Intellectual Property: Law and Policy* 181.

³⁷⁴ See WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 27; WIPO Standing Committee on the Law of Patents, “Report on the International Patent System” SCP/12/3 Rev.2, Revised Annex II; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 19.

³⁷⁵ Dutch Patent Act, art 53(3).

³⁷⁶ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 27.

³⁷⁷ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 27.

ucts case that “both society and the scientist have a ‘legitimate interest’ in using the patent disclosure to support the advance of science and technology”.³⁷⁸ The exemption though is not absolute. While “the research exemption applies to research on or into a patented invention, for example, working on the patented invention in order to explore unknown effects or further develop the invention”, it does not normally cover “research made with the patented invention”.³⁷⁹ The scientific research exemption therefore permits experiments on the patented invention but not the use of the invention in contexts outside of such experiments. In any event, the scientific research exemption is a boon to makers and hacktivists as they are able to openly examine, experiment on and even improve patented technologies. They can perform all of the common acts of hacking on a patented technology – explore, break, learn, create, share and secure. In contrast to the private copying and use exception where sharing is impeded, hackers as researchers have a greater ability to share and communicate what they have learned about a patented invention since the grant of a patent is predicated on the public disclosure and transparency about how the invention works.³⁸⁰ The scientific research exemption thus advances a number of hacker norms and values such as openness, freedom of access, transparency, curiosity, creativity and innovation, efficiency, community development, and social development.

4.3.3.5 Repair of equipment

The Copyright Directive contains an exception to reproduce or use a copyrighted work “in connection with the demonstration or repair of equipment”.³⁸¹ This exception is akin to the right to use software under the Software Directive, where a lawful user or possessor

³⁷⁸ Canada - Patent Protection of Pharmaceutical Products, WT/DS114/R (17 March 2000) para 7.69; see also WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 27.

³⁷⁹ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 29.

³⁸⁰ But see Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 19 and 21 (on limitations on sharing like commercial use).

³⁸¹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(3)(l).

can perform acts necessary to use a protected work, including correcting errors or repairing technical issues. In the United States, a right to repair whether involving copyright or patents has been recognized by courts.³⁸² This right to repair protects hackers and ordinary users “especially those who engage in this activity for noncommercial purposes”.³⁸³ This exception is especially pertinent to makers because they prefer to use and work with technologies and equipment that are repairable.³⁸⁴

4.3.3.6 Fair use and the three-step test

Fair use is possibly one of the most useful and powerful limitations and exceptions to copyright.³⁸⁵ However, this legal doctrine is only adopted and followed in the United States and a few other jurisdictions such as Israel, Korea, Liberia, the Philippines, Sri Lanka, Taiwan and Uganda.³⁸⁶ It is generally not adhered to in Europe, including the Netherlands.³⁸⁷ While some European countries have the concepts of “fair dealing” or “fair practice”, these should not be confused with fair use as they only apply in specific cases and they are not as flexible and robust in adapting to techno-social changes as the latter.³⁸⁸ For instance, a country in Europe would have to amend its national laws to recognize the lawfulness of the widely accepted practice of users ripping music CDs to play music on their portable devices.³⁸⁹

³⁸² See Pamela Samuelson, “Freedom to Tinker” 22 (citing *Wilson v Simpson*, 50 U.S. (9 How.) 109 and *Bureau of Nat’l Literature v Sells*, 211 F. 379 (W.D. Wash. 1914).

³⁸³ Pamela Samuelson, “Freedom to Tinker” 22.

³⁸⁴ See “Repair Manifesto” and “Self-Repair Manifesto”.

³⁸⁵ See Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 38.

³⁸⁶ See Jonathan Band and Jonathan Gerafi, “The Fair Use/Fair Dealing Handbook” 1; see also Christophe Geiger, Daniel Gervais and Martin Senffleben, “The Three-Step Test Revisited” 623-624.

³⁸⁷ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 67; Martin Senffleben, “Bridging the Differences Between Copyright Legal Traditions - The Emerging EC Fair Use Doctrine”; Jonathan Band and Jonathan Gerafi, “The Fair Use/Fair Dealing Handbook” 1; Martin Senffleben, “Fair Use in The Netherlands - a Renaissance?” 1.

³⁸⁸ Hector MacQueen and others, *Contemporary Intellectual Property* 179; *Berne Convention*, arts 10(1) and 10(2); Jonathan Band and Jonathan Gerafi, “The Fair Use/Fair Dealing Handbook” 1.

³⁸⁹ UK Intellectual Property Office, “Exceptions to copyright: An Overview”; *British Academy of Songwriters, Composers and Authors Musicians’ Union v Secretary of State for Business, Innovation and Skills* [2015] EWHC 2041 (Admin) (17 July 2015) (in the case of the United Kingdom, while an amendment to the law was passed, it was subsequently struck down by the courts).

Fair use represents the first of two differing approaches to establishing limitations and exceptions to copyright. They can either be “(i) open-ended, formulaic provisions, and (ii) ‘closed lists’”.³⁹⁰ The fair use doctrine is a prime example of the open-ended approach. Under US law, specifically section 107 of the US Copyright Act 1976, four factors are considered in determining whether a reproduction or use of a copyrighted work is an excepted fair use:

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.³⁹¹

The open-ended formulation of the fair use doctrine means that it has to be applied on a case-by-case basis. What this approach sacrifices with regard to legal certainty and consistency,³⁹² it makes up for with its “obvious advantage of flexibility” and responsiveness to socio-technical advances, which “enables new kinds of uses to be considered as they arise, without having to anticipate them legislatively”.³⁹³ This flexibility permits courts to adjust or adapt “the scope of limitations” of intellectual property rights “to new circumstances and challenges, such as the digital environment. Leaving this discretion to the courts reduces the need for constant amendments to legislation that may have difficulty in keeping pace with the speed of technological

³⁹⁰ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 67; see also Martin Senfileben, “The Emerging EC Fair Use Doctrine” 548.

³⁹¹ US Copyright Act 1976, section 107; see also *Folsom v Marsh* (1841); see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 38.

³⁹² Martin Senfileben, “The Emerging EC Fair Use Doctrine” 527 and 529; Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 36.

³⁹³ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 68; see also Martin Senfileben, “The Emerging EC Fair Use Doctrine” 527.

development”.³⁹⁴ As Ginsburg notes, “The fair use exception permits a variety of unauthorized reproductions or derivative works, sometimes even for commercial purposes”.³⁹⁵ The application of the fair use doctrine in the United States has bolstered many groundbreaking and disruptive technical innovations and cultural practices such as video-cassette recorders and the time-shifting of television watching, digital music players and the place-shifting of music listening, internet search engines and the indexing of the Web, and book scanning and indexing by libraries.³⁹⁶

The open-ended style of fair use in the United States sharply contrasts with the closed list approach to copyright limitations and exceptions in Europe as expressed in Article 5 of the Copyright Directive.³⁹⁷ The Copyright Directive contains an exclusive and exhaustive list of limitations and exceptions to the rights of authors and copyright holders.³⁹⁸ While this approach offers greater clarity and legal certainty about the rights and obligations of parties to a protected work,³⁹⁹ it lacks the flexibility and dynamism of fair use. Under the closed list approach, if a new technology is developed and new cultural practices emerge (or vice versa), their lawfulness is judged based on whether they fall within the existing statutory limitations and exceptions, which as seen above are not plentiful and are strictly and narrowly applied. This is one of the underlying reasons why intellectual property rights and socio-technical innovations have such a fraught history: the former relies on the solidity and consistency of law whereas the latter flourishes with technical disruption and social change. The open-ended style of fair use appears better suited than the closed list approach to adapt

³⁹⁴ Martin Senfileben, “The Emerging EC Fair Use Doctrine” 527.

³⁹⁵ Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1616.

³⁹⁶ *Sony v. Universal* 464 U.S. 417 (1984); *Recording Industry Association of America v. Diamond Multimedia Systems* 180 F.3d 1072 (1999); *Field v. Google* 412 F.Supp.2d 1106 (2006); *Authors Guild v. Hathitrust* 755 F.3d 87 (2014); see also Lawrence Lessig, *Code: version 2.0* 184 and 187; see also Pamela Samuelson, “Hacking Intellectual Property Law” 67.

³⁹⁷ See Martin Senfileben, “The Emerging EC Fair Use Doctrine” 522 and 528.

³⁹⁸ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5 and recital 32.

³⁹⁹ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 72-73.

to rapid and ever increasing techno-social change that is a distinctive feature of living in the networked society.

While the concept of fair use may not exist in European copyright laws, it can be argued that the Copyright Directive already contains a key principle in intellectual property laws that is as robust as the fair use doctrine and may potentially be applied in a similarly flexible manner. At the end of the enumerated list of limitations and exceptions in the Copyright Directive, there is an important proviso that states: “The exceptions and limitations provided... shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder”.⁴⁰⁰ This proviso reproduces the so-called “three-step test” originally found in the Berne Convention.⁴⁰¹ The three-step test requires that a statutorily granted limitation or exception must: (1) apply only “in certain special cases”; (2) “does not conflict with a normal exploitation of the work”; and (3) “does not unreasonably prejudice the legitimate interests of the author”.⁴⁰² The three-step test is a “general formula” used to assess whether an existing or proposed statutory limitation or exception to the reproduction right is in accordance with the policies and objectives of intellectual property laws.⁴⁰³ It generally “operates as an overriding requirement” in assessing the validity of any limitation or exception.⁴⁰⁴ In order to comply with the test, national legislators must “provide reasonably narrow exceptions (a quantitative component),⁴⁰⁵ with a well-defined public interest justification (the normative/qualitative

⁴⁰⁰ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(5); Berne Convention, art 9(2); see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 34-35.

⁴⁰¹ Berne Convention, art 9(2); see also Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 21; WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 8.

⁴⁰² Berne Convention, art 9(2).

⁴⁰³ Berne Convention, art 9(2); see also Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 21; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 4.

⁴⁰⁴ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 72; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 23 and 34.

⁴⁰⁵ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 31.

component)”. The three-step test was “intended to serve as a flexible balancing tool offering national policy makers sufficient breathing space to satisfy economic, social, and cultural needs”.⁴⁰⁶

While it is not a specific limitation or exception to copyright *per se*,⁴⁰⁷ I agree with other scholars that the three-step test as stated in the Berne Convention and other international laws could be treated as being akin to the fair use doctrine and may likewise be applied as an open-ended standard to determine whether a specific or actual use of a protected work is legitimate or permissible.⁴⁰⁸ What is interesting about the three-step test is that, unlike the fair use doctrine, it applies not just to copyright but also to other intellectual property rights such as patent, database, and design rights.⁴⁰⁹ According to the WIPO, “Originally a test of limited application under Berne, it has now been adopted as a general template for limitations and exceptions under the TRIPS Agreement, the WCT and the WPPT”.⁴¹⁰ The test is “emerging as an unavoidable norm in copyright law but also in other areas of intellectual property”.⁴¹¹ Being such an encompassing and influential principle,⁴¹² it may be contended that the three-step test can serve as a standard not only for evaluating the validity of existing or proposed statutory limitations and exceptions, but also the legitimacy of all manner of possible uses of protected works and inventions.⁴¹³

⁴⁰⁶ Christophe Geiger, Daniel Gervais and Martin Senfileben, “The Three-Step Test Revisited” 582.

⁴⁰⁷ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 3, 20, 22 and 65.

⁴⁰⁸ Berne Convention, art 9(2); see Martin Senfileben, “The International Three-Step Test: A Model Provision for EC Fair Use Legislation”; see Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35 and 39; see Christophe Geiger, Daniel Gervais and Martin Senfileben, “The Three-Step Test Revisited” 582; see Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 23.

⁴⁰⁹ Agreement on Trade-Related Aspects of Intellectual Property Rights, arts 26 (industrial designs) and 30 (patents); Directive 2009/24/EC on the legal protection of computer programs, recital 15 and art 6(3) (computer programs); Directive 96/9/EC on the legal protection of databases, arts 6(3) and art 7(5) (databases); see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35 and 38.

⁴¹⁰ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 65; Agreement on Trade-Related Aspects of Intellectual Property Rights, arts 13 and 30; WIPO Copyright Treaty, art 10; WIPO Performances and Phonograms Treaty, art 16; see also Martin Senfileben, “The Emerging EC Fair Use Doctrine” 544.

⁴¹¹ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 38.

⁴¹² Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 20 (the three-step test “has now come to enjoy something of the status of holy writ”); see also Christophe Geiger, Daniel Gervais and Martin Senfileben, “The Three-Step Test Revisited” 586 and 625.

⁴¹³ See Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 38.

Applying the three-step test in this way offers tremendous benefits to makers and hackers since their inherently innovative technologies and practices can be weighed and assessed from a more practical and policy-oriented perspective rather than the strict application of rigid and closed limitations and exceptions to exclusive intellectual property rights. This proposal is explored and expanded some more in Section 6.3.2.

4.4 Contract and anti-circumvention laws

Despite some of the liberty and autonomy offered by the limitations and exceptions to copyright and patents laws and the exploitable gaps and loopholes in computer crime laws discussed above, the ability of makers and hackers to hack are often further suppressed by and through contracts and anti-circumvention mechanisms. Working in conjunction with computer crime, intellectual property and anti-circumvention laws, these private contractual arrangements and technological protection measures act as a hybrid regime of techno-legal rules that are wont to impede various forms and acts of hacking. The use of restrictive contractual provisions and technological constraints can expand and magnify the rights and control of owners and creators over their information systems or intellectual creations because, under computer crime and intellectual property laws, the lawfulness or legitimacy of most forms of access or use fundamentally hinges on the presence or absence of authorization or permission from the owner or creator. Owners and creators therefore possess and wield much discretion and power in determining who can access and use their information and technologies, in what manner such access and use is carried out, and, most critically, what laws apply (including whether or when the law has been breached). As explained below, this state of affairs has a palpably negative effect on hacking.

4.4.1 CONTRACTS

4.4.1.1 Contractual terms and conditions

Contracts are essentially private yet legally binding agreements that are consented or entered into by and between parties that set out their rights and obligations with regard to a specific subject matter.⁴¹⁴ Pursuant to the principles of freedom of contract and party autonomy, the contracting parties have the ability to decide for themselves the terms and conditions of their agreement.⁴¹⁵ Contracts represent the private law between the parties,⁴¹⁶ and the law and legal institutions will generally recognize, uphold and enforce such contractual stipulations and arrangements, unless there is a specific or exceptional ground under the law to rescind, annul or declare the entire contract or a contractual provision unlawful, unenforceable or void.⁴¹⁷ This ability or freedom to contract enables parties to enter into and perform all sorts, forms and manner of private arrangements and stipulations, which, in turn, shapes and pervades all aspects of social and economic life. Specifically in relation to intellectual property, De Werra explains that:⁴¹⁸

Contract law has always played an essential role in the system of copyright law because contracts have been the usual vehicle by which copyrighted works have been put to use. Authors have generally licensed or transferred one or several of the rights in their works to intermediary entities that subsequently distributed those works to the public. In all the specialized markets that have developed around the various types of protected works, the basic rule has always been freedom of contract.⁴¹⁹

⁴¹⁴ Niva Elkin-Koren, "Copyright policy and the limits of freedom of contract" 107-108.

⁴¹⁵ Raymond Nimmer, "Breaking barriers: the relations between contract and intellectual property law" 878; see Kurt Opsahl and Pamela Samuelson, "Licensing information in the global information market: freedom of contract meets public policy"; see Jacques De Werra, "Moving beyond the conflict between freedom of contract and copyright policies".

⁴¹⁶ Lawrence Lessig, Code: version 2.0 187.

⁴¹⁷ Michael Dizon, "The symbiotic relationship between global contracts and the international IP regime" 560; Jacques De Werra, "Moving beyond the conflict between freedom of contract and copyright policies"; Lawrence Lessig, Code: version 2.0 187.

⁴¹⁸ Raymond Nimmer, "Breaking barriers: the relations between contract and intellectual property law" 832; Michael Dizon, "The symbiotic relationship between global contracts and the international IP regime" 561.

⁴¹⁹ Jacques De Werra, "Moving beyond the conflict between freedom of contract and copyright policies" 246-247; see also Daniel Gervais, "A Principled Approach to Copyright Exceptions and Limitations" 16/

Technology and intellectual property contracts can take the form of standard boilerplate contracts and licensing agreements such as end-user license agreements (EULAs), non-disclosure agreements (NDAs), website terms of service, “shrink-wrap licences, click-through or click-wrap agreements, access contracts” and other terms of use.⁴²⁰ In the context of the networked information society, it is virtually impossible to imagine a situation where contracts and contract law do not apply. It is no wonder then that contracts are considered “the principal instrument for legal innovation and legal standardization”, as well as the foremost means by which the terms and conditions for accessing and using information and technologies are set.⁴²¹

4.4.1.2 Freedom and restraints of contract

It should be noted though that there is a crucial condition that undergirds freedom of contract. Freedom of contract is based on the assumption that the parties freely negotiated and consented to the terms of the contract because they had more or less equal bargaining positions or stood on a relatively level playing field.⁴²² But this is not normally the case when it comes to matters relating to access and use of information, technology and intellectual property where the bargaining power of the contracting parties is most often asymmetric and lopsided. As seen in relation to intellectual property rights, it is the owners or creators who usually have a dominant bargaining position and can set the terms and conditions that are most advantageous to them. In most cases, users, consumers and hackers alike have to agree to contracts of adhesion (with their long list of provisions and impenetrable language), which are drafted by and for the benefit the owners and creators and much be accepted on a “take it or leave it” basis.⁴²³ It is true

⁴²⁰ Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 559 and 560; see also Michael Madison, “Legal-ware: contract and copyright in the digital age” 1032.

⁴²¹ Nicola Lucchi, “The supremacy of techno-governance” 214.

⁴²² Niva Elkin-Koren, “Copyright Policy and the Limits of Freedom of Contract” 108-109.

⁴²³ Llewellyn Joseph Gibbons, “Social Enforcement or Social Contracting for Governance of Cyberspace” 531; see J.H. Reichman and Jonathan Franklin, “Privately legislated intellectual property rights”.

that, in theory, users (including makers and hacktivists) still have the option of not using a particular information system or protected work. However, the pervasiveness, embeddedness and essentiality of certain information technology and intellectual property in daily life and the lack of viable alternatives render such a choice moot.⁴²⁴ Whether its listening to music, reading an ebook, joining a social networking site, reading news online, downloading an app, conducting a web search, or even using a smartphone or computer, many common activities and most popular or dominant information and technology products and services (e.g., iTunes, the Kindle Store, Facebook, the Apple App Store, Google, Android, or Windows) require people to assent to more or less restrictive licenses or terms of use. How reasonable or feasible would it be for someone who wants to genuinely participate and be involved in the information society to refuse to use those products and services and reject their contractual terms or licenses?

In addition to hackers' and ordinary users' lack of genuine bargaining power and ability to negotiate, what is especially egregious about the technology and intellectual property contracts commonly used today (with the exception of free and open licenses) is that they are a means through which people waive or bargain away through contract even the few existing rights, opportunities and freedoms that they have under the law.⁴²⁵ This is legally possible and permissible because, aside from a few instances, there is no explicit prohibition under the law that bars parties from contracting away their legal rights and privileges.⁴²⁶ Under intellectual property laws,

Subject to discrete exceptions and qualifications..., the general rule is that the initial endowment of rights and obligations... may be subsequently modified, transferred, limited, suppressed, waived, disposed of, or bargained away by contracts or through

⁴²⁴ See Ronald Leenes, "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology" 165.

⁴²⁵ Lawrence Lessig, Code: version 2.0 187.

⁴²⁶ See WIPO Standing Committee on Copyright and Related Rights, "Updated Report on the Questionnaire on Limitation and Exceptions" SCCR/21/7 11.

voluntary agreements between parties following the principle of freedom of contract.⁴²⁷

Save for the specific cases of reverse-engineering, decompilation and making back-up copies, the other limitations and exceptions to intellectual property rights that apply to makers and hacktivists can be waived or diminished through contracts.⁴²⁸ Contracts have the ability “to rewrite the balance that copyright law creates”.⁴²⁹ For instance, “copyright owners have... used contractual restrictions to augment copyright limits on user modifications to their copies of protected works”.⁴³⁰ Private contractual arrangements can also be used to “control and delimit all possible ways by which a user may use the licensed software by imposing a multitude of obligations and restrictions that exceed those set under the applicable IP laws”.⁴³¹ The combination of exclusive intellectual property rights with overly restrictive contracts produces what is tantamount to “privately legislated intellectual property rights’ that override public policy and default rules on IP as contained in international and national IP laws”.⁴³²

While it is true that the FOSS movement, through the use of copyleft licenses, defensive patent publications, and other creative-subversive techno-legal tactics, has acted as a valuable counterbalance to the maximalist approach and restrictive application of contractual provisions in relation intellectual property,⁴³³ the misapplication or

⁴²⁷ Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 560; see also Niva Elkin-Koren, “Copyright policy and the limits of freedom of contract” 105.

⁴²⁸ Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 560; Jacques De Werra, “Moving beyond the conflict between freedom of contract and copyright policies” 322; James Maxeiner, “Standard-terms contracting in the global electronic age” 134-141.

⁴²⁹ Lawrence Lessig, Code: version 2.0 187.

⁴³⁰ Pamela Samuelson, “Freedom to Tinker” 10.

⁴³¹ Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 562; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 25.

⁴³² Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 560; see also J.H. Reichman and Jonathan Franklin, “Privately legislated intellectual property rights” 878; see also Kurt Opsahl and Pamela Samuelson, “Licensing information in the global information market: freedom of contract meets public policy” 390; see also Lawrence Lessig, Code: version 2.0 (on the “race to privatize copyright law through contract”).

⁴³³ See Michael Dizon, “The symbiotic relationship between global contracts and the international IP regime” 561-563; see Beth Noveck, “Peer to Patent’: Collective Intelligence, Open Review, and Patent Reform”; see Jason Schultz and Jennifer Urban, “The Defensive Patent License as New Approach to Patent Threats”; see Open Invention Network, “Defensive Publications” <<http://www.defensivepublications.org/>> accessed on 9 December 2014; see Andrew Katz, “Towards a Functional Licence for Open Hardware”;

abuse of freedom of contract remains the standard practice among many corporate and commercial owners and creators of information systems and intellectual property, and the private legal arrangements they impose serve as barriers to hacking since these generally tend to impede rather than promote free and open access to and creative uses of information and technology, which lies at the core of hacking projects and activities. Unlike computer crime laws (which generally concern what technologies and systems can be the targets of hacking), contract law affects what tools hackers can use for hacking.

4.4.1.3 Contracts and computer crime

A similarly troublesome situation exists when restrictive contracts and computer crime laws are applied together. The owners and creators of computer systems and data can contractually stipulate what users can or cannot do. While it is well within their rights to exert as much control over their technologies based on their general right of ownership, contractual restrictions when pushed to the extreme and enforced together with computer crime laws become highly problematic and of questionable legitimacy because they threaten “to put the immense coercive power of criminal law in the hands of those who draft contracts”.⁴³⁴ As argued by the Electronic Frontier Foundation, “violating a private agreement or duty should not carry the grim shadow of criminal liability”, but the reverse seems to be the general tendency or outcome when restrictive contractual agreements work hand in hand with computer crime laws.⁴³⁵ It is worth recalling that access or use without right or authority is a common element in the first four computer security crimes. Since a user’s right or authority to use or access most technologies or intellectual property rights is founded or predi-

see Open Source Hardware Association, “Open Source Hardware (OSHW) Statement of Principles 1.0” <<http://www.oshwa.org/definition/>> accessed on 9 December 2014.

⁴³⁴ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3; see also Christine Galbraith, “Access Denied” 338 and 365; see also Cassandra Kirsch, “The Grey Hat Hacker” 399.

⁴³⁵ Marcia Hofman and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; see also Christine Galbraith, “Access Denied” 323.

cated on an existing contractual agreement or license, then a breach of contract can also result in a violation of criminal law.⁴³⁶

In a growing number of cases especially in the United States, public prosecutors and some courts have taken the view that the crime of illegal access can apply to breaches of contractual terms and conditions and employment agreements.⁴³⁷ The rationale behind this interpretation is that once a user or an employee breaches the agreed terms of use, their access to the relevant information system has become without or in excess of their authority.⁴³⁸ In the United States, for instance, public prosecutors have filed criminal charges against ordinary users and employees for using a computer system in excess of their authority.⁴³⁹ Their expansive construction of the law “threaten[s] to criminalize any breach of contract or employee disloyalty involving computers”.⁴⁴⁰ Most courts have disagreed with this overzealous interpretation of the law and have refused to hold ordinary users criminally liable for simply breaching standard terms of use or service.⁴⁴¹ In the cases where the courts found employees guilty of the crime of illegal access, there was evidence of actual or intent to cause harm or damage.⁴⁴² While it is true that courts have on the whole interpreted and applied the illegal access provision reasonably and judiciously and public prosecutors may be given the benefit of the doubt to not abuse their discretion⁴⁴³ in prosecuting minor cases or trivial activities,⁴⁴⁴

⁴³⁶ Christine Galbraith, “Access Denied” 338.

⁴³⁷ Parker Higgins, “Critical Fixes for the Computer Fraud and Abuse Act”; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1598; Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3-4.

⁴³⁸ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3.

⁴³⁹ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3-4.

⁴⁴⁰ Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1601.

⁴⁴¹ Parker Higgins, “Critical Fixes for the Computer Fraud and Abuse Act”; Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3.

⁴⁴² Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3-4; see Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes”.

⁴⁴³ See Bert-Jaap Koops, “Cybercrime Legislation in the Netherlands” 3 (on the Dutch public prosecutor’s “prosecutorial discretion” to decide what acts are “worthy of criminal prosecution”).

⁴⁴⁴ See Orin Kerr, “Vagueness Challenges to the Computer Fraud and Abuse Act” 1562, 1578, 1579; see Cyrus Chung, “The Computer Fraud and Abuse Act” 233-234; see Cindy Cohn, Hammi Fakhoury and Marcia Hofman, “Rebooting Computer Crime Law Part 3”.

these are not acceptable reasons or “justification[s] for ignoring fundamental flaws in the statute” such as the problematic definition of illegal access and its misapplication in relation to contract law.⁴⁴⁵ As a US Court of Appeals ruled in the case of *US v Valle*, where an employee was criminally prosecuted under the US Computer Fraud and Abuse Act for violating the employer’s computer use policy:

While the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters. A court should not uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly.⁴⁴⁶

Applied in conjunction with restrictive contracts, the illegal access provision hangs as a veritable sword of Damocles over the heads of all users and consumers of technological products or services where certain uses are not expressly permitted in the relevant contract, agreement or license by the owners, producers or providers of the technology or information system.⁴⁴⁷ Even if it is argued that the threat is mainly theoretical, there is something particularly egregious about the idea that “private parties, rather than lawmakers, would be in a position to determine what conduct is criminal – simply by prohibiting it in an agreement”.⁴⁴⁸ It is a basic principle of law that a breach of contract is subject to civil not criminal liability.⁴⁴⁹ While it is true that “without right” is an element of many other crimes, the unique nature and characteristics of information, computer data and digital technologies make the commission of a crime like illegal access and the trigger-

⁴⁴⁵ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 605.

⁴⁴⁶ *United States v Gilberto Valle*, No. 1402710ler and No. 1404396ler (3 December 2015).

⁴⁴⁷ Marcia Hofman and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 2, 3 and 5; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1640.

⁴⁴⁸ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3; see also Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1650 and 1651.

⁴⁴⁹ E. Allan Farnsworth, “Legal Remedies for Breach of Contract” 1145-1146; William McBryde, “Remedies for Breach of Contract” 75; Avery Katz, “Remedies for breach of contract under the CISG” 378-379; see also William Bishop, “The Choice of Remedy for Breach of Contract”.

ing of criminal liability for a breach of contract far too easy or trivial to commit.

Criminalizing terms of service violations is all the more troubling given that these terms are contained in contracts of adhesion, which are non-negotiable and “often vague, lopsided and subject to change without notice”.⁴⁵⁰ Since almost all information and technology products, services and systems nowadays are subject to contractual licenses and conditions, hackers as well as users who creatively use or access any of these technologies or content can be subjected to criminal prosecution for simply violating a private agreement. The problem with vague laws is that they are “dangerous precisely because they give prosecutors and courts too much discretion to arbitrarily penalize normal, everyday behavior”.⁴⁵¹

It is good to note though that EU legislators hold the position that the mere violation of contractual terms and conditions should not trigger the application of computer crime laws. The Cybercrime Directive expressly states that:

contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards access to and use of information systems of an employee for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings.⁴⁵²

While this statement is contained in a recital, “the preamble... serves as a guideline for the interpretation of the operative part of the text”⁴⁵³ and has a controlling effect on the enforcement of the Direc-

⁴⁵⁰ Marcia Hofman and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 3; see also Parker Higgins, “Critical Fixes for the Computer Fraud and Abuse Act”.

⁴⁵¹ Marcia Hofman and Rainey Reitman, “Rebooting Computer Crime Law Part 1”; Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1599.

⁴⁵² Council Directive 2013/40/EU on attacks against information systems, recital 17.

⁴⁵³ See Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 34.

tive. Moreover, even though the preamble is not a source of rights and obligations per se, it may serve as a legal basis or reason for courts and other public authorities in interpreting or deciding on the applicability of the Directive's provisions.

4.4.2 ANTI-CIRCUMVENTION RULES

4.4.2.1 Technological protection measures

Apart from contracts, the rights and obligations under intellectual property and computer crime laws (most notably the power of owners and creators to control access to and use of their information and technologies) can be greatly modified and expanded through technical means such as copy protection mechanisms, digital rights management (DRM), rights management information and other technological measures. Rights holders, for instance, can use DRM “to restrict a user’s access to and control of digital content”.⁴⁵⁴ The legal regime that protects and prohibits the circumvention of these technological protection measures is founded on the anti-circumvention provisions of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, otherwise known as the WIPO Internet Treaties.⁴⁵⁵

Under the WIPO Internet Treaties, contracting state parties are obliged to provide “adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their” copyright and related rights.⁴⁵⁶ Technological measures can take the form of “devices that prevent access to a work except on certain conditions, or copy-protection or other devices that restrict or prevent various infring-

⁴⁵⁴ Declan McCullagh and Milana Homsí, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 318; see also Michael Dizon, “Participatory democracy and information and communications technology” 14.

⁴⁵⁵ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2.

⁴⁵⁶ WIPO Copyright Treaty, art 11; WIPO Performances and Phonograms Treaty, art 18.

ing uses”.⁴⁵⁷ In addition, states are required to “provide adequate and effective legal remedies against” certain acts that may “induce, enable, facilitate or conceal an infringement” of the exclusive rights of authors and creators.⁴⁵⁸ The prohibited acts are: removing or altering “any electronic rights management information without authority”;⁴⁵⁹ and distributing, importing for distribution, broadcasting or communicating “to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority”. Rights management information is defined under the treaties as any “information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information” that “is attached to a copy of a work or appears in connection with the communication of a work to the public”.⁴⁶⁰

The Copyright Directive, which incorporates the anti-circumvention provisions of the WIPO Internet Treaties into EU law, makes the act of circumventing technological measures illegal, but subject to the qualification that the “person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective”.⁴⁶¹ Furthermore, the acts related to distribution and public communication must be carried out for “commercial purposes”.⁴⁶² A circumvention technology, information or activity falls within the prohibition if it is either: (a) “promoted, advertised or marketed for the purpose of circumvention”, (b) of “only a limited commercially significant purpose or use other than to circumvent”, or (c) “primarily

⁴⁵⁷ WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 81.

⁴⁵⁸ WIPO Copyright Treaty, art 12(1); WIPO Performances and Phonograms Treaty, art 19(1).

⁴⁵⁹ WIPO Copyright Treaty, art 12(1)(i) and (ii); WIPO Performances and Phonograms Treaty, art 19(1)(i) and (ii).

⁴⁶⁰ WIPO Copyright Treaty, art 12(2); WIPO Performances and Phonograms Treaty, art 19(2); see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 7(2).

⁴⁶¹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, arts 6(1) and 7(1); see also Dutch Copyright Act, art 29a(2); see also WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 9.

⁴⁶² Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 6(2).

designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention” of any “effective technological measure”.⁴⁶³ Under the Directive, a “technological measure” is defined as “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter” that is “not authorized by the rightholder” or under law, and it is considered “effective” if, “through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter”, the protection objective is achieved.⁴⁶⁴ The Copyright Directive also makes it illegal for any person to remove or alter any electronic rights-management information, or to distribute or make available to the public protected works and subject-matter whose “electronic rights-management information has been removed or altered without authority”.⁴⁶⁵ This legal prohibition is subject to the proviso that “such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright”.⁴⁶⁶ In the Netherlands, the anti-circumvention provisions are contained in the Dutch Copyright Act and they hew closely to the Copyright Directive.⁴⁶⁷

Whether pursuant to the WIPO Internet Treaties or their different regional or national law implementations, the anti-circumvention provisions essentially outlaw three activities: (1) breaking or defeating technological measures that protect and set the terms and limits of access and use of information and technology placed by the owners or creators; (2) distributing or communicating to the public technologies

⁴⁶³ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 6(2)(a), (b) and (c).

⁴⁶⁴ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 6(3); see also Dutch Copyright Act, art 29a(1); see also European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 8 (on a Finnish court’s interpretation of effective); see also Michael Dizon, “Participatory democracy and information and communications technology” 14; see also Declan McCullagh and Milana Homsy, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 318.

⁴⁶⁵ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 7(1).

⁴⁶⁶ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 7(1).

⁴⁶⁷ Dutch Copyright Act, art 29a.

or information about circumvention; and (3) distributing or making available to the public protected works whose technological measures or rights management information have been removed.⁴⁶⁸ It should be noted though that with respect to technological measures concerning computer programs it is the specific provisions of the Software Directive and not the Copyright Directive that apply.⁴⁶⁹ This means that in Europe anti-circumvention rules do not apply to acts of reverse engineering or decompilation software.⁴⁷⁰ Furthermore, it appears that circumventing technological protection measures for the purpose of reverse engineering or decompiling a computer program is considered lawful and cannot be waived or defeated by contract.⁴⁷¹ This is tremendously beneficial to makers and hackers since two of the primary reasons why they break the DRM on a computer program are either to enable them to understand how it works or to make the program interoperable with other software, content or data.⁴⁷² It should be noted though that outside of Europe, the anti-circumvention laws of some countries restrict or “outlaw most reverse engineering (‘circumvention’) of technically protected copyrighted works and the making or offering of tools to enable such reverse engineering”.⁴⁷³

The adoption of anti-circumvention laws was admittedly well intentioned. According to WIPO, the WIPO Internet Treaties and their anti-circumvention provisions were meant to “address the challenges posed by today’s digital technologies, in particular the dissemination

⁴⁶⁸ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, arts 6(1)-(2) and 7(1); see also Michael Dizon, “Participatory democracy and information and communications technology” 15; see also WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 82; see also WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 3; see also Michael Dizon, “Does Technology Trump Intellectual Property?” 131.

⁴⁶⁹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 50; see also Dutch Copyright Act, art 32a; see also Pamela Samuelson, “Anticircumvention Rules: Threat to Science” 2028.

⁴⁷⁰ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 50.

⁴⁷¹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 50; Directive 2009/24/EC on the legal protection of computer programs, arts 5(3), 6 and 8.

⁴⁷² See Phillip Torrone, “Sony’s War on Makers, Hackers, and Innovators” (the case of George Hotz breaking the security of the Playstation 3 to run his own games and software on the device); see Kristin Eschenfelder, Robert Howard and Anuj Desai, “A Content Analysis of Web Sites Posting DVD Circumvention Software” 1408 (Jon Johansen defeating the copy-protection on DVDs so he could watch movies on his Linux computer); see also Electronic Frontier Foundation, “Unintended Consequences: Fifteen Years under the DMCA”.

⁴⁷³ Pamela Samuelson, “Freedom to Tinker” 3.

of protected material over digital networks such as the Internet”.⁴⁷⁴ As with other amendments and revisions to intellectual property laws, the anti-circumvention rules were primarily a response to “developments in technology and in the marketplace”.⁴⁷⁵ There was a fear that “digital technology” would “undermine the basic principles of copyright and related rights” and lead to the “disruption of traditional markets for the sales of copies of computer programs, music, art, books and movies”.⁴⁷⁶ The drafters of the WIPO Internet Treaties believed that, in the digital networked environment, intellectual property rights could not be “applied efficiently without the support of technological measures of protection and rights management information necessary to license and monitor uses”.⁴⁷⁷ While “[t]here was agreement that the application of such measures and information should be left to the interested rights owners”, the drafters still deemed it necessary that “appropriate legal provisions were needed to protect the use of such measures and information”.⁴⁷⁸ In relation to preserving the intellectual property balance, the underlying rationale was that, by giving authors and creators greater legal protection and control over their works, they would be incentivized to make their works publicly and widely available in digital format and on information networks.⁴⁷⁹ The expressed policy reasons behind anti-circumvention laws were both economic and social.⁴⁸⁰ While the law was meant to “sustain the national copyright

⁴⁷⁴ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2 and 3; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 4; see also WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 4; see also Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1618; see WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 11-12.

⁴⁷⁵ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2.

⁴⁷⁶ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 5; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 9 and 10.

⁴⁷⁷ WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 7.

⁴⁷⁸ WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 7; see also WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 3.

⁴⁷⁹ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 78; Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1618.

⁴⁸⁰ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 78.

industries, attract investment, and protect local creativity”,⁴⁸¹ there was also recognition that “it was necessary to maintain a balance between these rights and the ‘larger public interest,’ particularly education, research and access to information”.⁴⁸² However, as explained below, anti-circumvention rules have proven to be ineffective against digital piracy and they have produced technical and legal barriers that inhibit legitimate users from reasonably accessing and using information and technologies.

4.4.2.2 Techno-legal barriers

Despite their laudable objectives, anti-circumvention laws have proven to be extremely contentious and problematic.⁴⁸³ One of the primary aims of anti-circumvention laws is to prevent digital copyright infringement. But, in practice, it is hackers rather than intellectual property infringers and pirates who are inhibited by the law. Samuelson explains that hackers or tinkerers

who plan to make non-infringing uses of technically protected works are, oddly enough, more likely to be deterred by the anti-circumvention laws than those who tinker to infringe. After all, the payoff of infringement may be large, and it is often easy for destructive tinkerers to hide in the darknet. Constructive tinkerers, by contrast, tend to be more open about what they are doing and willing to explain why it is in society’s interest that they be free to tinker and share the results of what they’ve learned with the world.⁴⁸⁴

Further, while the WIPO claims that the WIPO Internet Treaties “reflect a broad international agreement as to how copyright and related rights should be handled... in the context of digital technologies”,

⁴⁸¹ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 4; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 2.

⁴⁸² Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 78; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recitals 3 and 31.

⁴⁸³ See WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 8.

⁴⁸⁴ Pamela Samuelson, “Freedom to Tinker” 16.

and “[t]he ultimate result has been widely acknowledged as balanced and fair”, this appears to be true only for those commercial authors, creators and others with vested interests who stand to directly benefit from these laws.⁴⁸⁵ In fact, the legitimacy and acceptance of anti-circumvention laws and technologies have been criticized and objected to “even at the time of the adoption of the WIPO Internet Treaties”.⁴⁸⁶ Contrary to what the WIPO asserts, anti-circumvention rules are neither reasonable nor balanced from the viewpoint of hackers and ordinary users,⁴⁸⁷ and they do not “help minimize the gap between the digital haves and have-nots”.⁴⁸⁸ The truth is, the combination of technological measures with legal prohibitions against circumvention has resulted in a hybrid regime of techno-legal rules that on two levels grants owners and creators more control over their information and technology that is beyond what is formally envisioned and expressly provided for under the law.⁴⁸⁹ This techno-legal regime of anti-circumvention “permits a much more fine-grained control over access to and use of protected material than the law permits, and it can do so without the aid of the law”.⁴⁹⁰ Furthermore, even though the WIPO Internet Treaties and the Copyright Directive recognize the importance of establishing limitations and exceptions to anti-circumvention rules (e.g., for cryptography research),⁴⁹¹ most countries have not made full use of this authority, and the few limitations and exceptions that exist are of strict and limited application.⁴⁹² To make matters worse, under

⁴⁸⁵ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 2 and 6; Michael Dizon, “Does Technology Trump Intellectual Property?” 131.

⁴⁸⁶ Michael Dizon, “Participatory democracy and information and communications technology” 16; see also Ian Brown, “The Evolution of Anti-Circumvention Law” 240-242.

⁴⁸⁷ Ian Brown, “The Evolution of Anti-Circumvention Law” 255; Declan McCullagh and Milana Homsí, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 326.

⁴⁸⁸ WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 10.

⁴⁸⁹ Michael Dizon, “Participatory democracy and information and communications technology” 15; Declan McCullagh and Milana Homsí, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 319; Jessica Litman, *Digital Copyright* 27; Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1619; Lawrence Lessig, *Code: version 2.0* 186.

⁴⁹⁰ Lawrence Lessig, *Code: version 2.0* 179; see also Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1631-1632.

⁴⁹¹ WIPO, *Agreed Statements concerning the WIPO Copyright Treaty 1996*; see Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 48 and art 5(2)(b); see Pamela Samuelson, “Anticircumvention Rules: Threat to Science” 2029.

⁴⁹² WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and

the law, even these limitations and exceptions can be waived or suppressed through contracts and technological measures.⁴⁹³

It comes as no surprise then that these anti-circumvention rules have produced negative effects and unintended consequences.⁴⁹⁴ There have been a number of documented cases of anti-circumvention laws and technologies adversely affecting “freedom of expression, privacy, competition law, academic research and consumer protection”.⁴⁹⁵ There is also a well-grounded fear that anti-circumvention rules could “allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work”.⁴⁹⁶ Technological measures have indeed been utilized to “curb fair use, limit access to materials that has passed out of copyright and into the public domain, work in consumer-unfriendly ways, and require disclosure of personal information that could raise privacy concerns”.⁴⁹⁷ While it is true that owners and creators have the right to adopt any technical, contractual, legal and other means at their disposal to protect their property,⁴⁹⁸ a balance must be struck and maintained by and in the law that equally recognizes and takes account of the legitimate interests of users and other social goals and values.

Exceptions” SCCR/21/7 12, 13 and 15; Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 51 and art 6(4); European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 9; Ian Brown, “The Evolution of Anti-Circumvention Law” 249; P. Akester and R. Akester, “Digital rights management in the 21st century” 161 and 165; see also Alvise Maria Casellati, “The Evolution of Article 6.4 of the European Information Society Copyright Directive” 397 (vagueness of limitations and exceptions); but see European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 7.

⁴⁹³ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 6(4); Dutch Copyright Act, art 29a(4); see also Severine Dusollier, “Exceptions and technological measures in the European Copyright Directive of 2001 - an empty promise” 71-72; see also Lucie Guibault, Guido Westkamp and Thomas Rieber-Mohn, “Study on the Implementation and Effect in Member States’ Laws on Directive 2001/29/EC” 112.

⁴⁹⁴ Electronic Frontier Foundation, “Unintended Consequences: Fifteen Years under the DMCA”; see also Ian Kerr, Alana Maurushat, Christian Tacit, “Technical Protection Measures: Tilting at Copyright’s Windmill” 68-75; see also Pamela Samuelson, “Anticircumvention Rules: Threat to Science” 2028; see also Michael Dizon, “Participatory democracy and information and communications technology” 14-15.

⁴⁹⁵ Ian Brown, “The Evolution of Anti-Circumvention Law” 240; see also Kristin Eschenfelder and Antij Desai, “Software as Protest: The Unexpected Resiliency of U.S.-Based DeCSS Posting and Linking” 102; Pamela Samuelson, “Anticircumvention Rules: Threat to Science” 2028.

⁴⁹⁶ *Chamberlain Group v Skylink Technologies* 381 F. 3d 1178 (2004), 1202; see also Lucie Guibault, Guido Westkamp and Thomas Rieber-Mohn, “Study on the Implementation and Effect in Member States’ Laws on Directive 2001/29/EC” 155.

⁴⁹⁷ Declan McCullagh and Milana Homsí, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” 319; see also Ronald Leenes, “Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology” 163-164.

⁴⁹⁸ See Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 52 and art 6(4).

The charges of illegitimacy and overbreadth that hound anti-circumvention rules is quite evident from the fact that some of their problematic uses do not even directly concern or relate to the prevention of intellectual property right infringement, which is the main purpose and stated objective of the law.⁴⁹⁹ Instances where anti-circumvention laws and rules have been applied and enforced even though they have nothing to do with copyright piracy include: a telephone company preventing users and others parties from unlocking mobile phones,⁵⁰⁰ a game developer company suing another company that produced a program that made playing a massively multiplayer online role-playing game (MMORPG) less tedious,⁵⁰¹ companies attempting to stave off the creation and introduction of more innovative or competing products and services in the market,⁵⁰² technology companies threatening or barring security researchers from disclosing security vulnerabilities,⁵⁰³ movie companies preventing users who lawfully purchased DVDs from format shifting,⁵⁰⁴ and car and tractor companies dissuading people from tinkering with or fixing their vehicles.⁵⁰⁵ Clearly, the above cases “pose virtually no risk of enabling infringement of commercially exploited copyrighted works.... TPMs [technological protection measures] are being used to thwart competition in certain industry sectors, with the anti-circumvention rules as reinforcements”.⁵⁰⁶

Anti-circumvention rules, whether of the technical, legal or hybrid variety, are the very antithesis of hacking because they produce a kind of “de facto access rights that do not only prohibit unautho-

⁴⁹⁹ See WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)” 8; Michael Dizon, “Does Technology Trump Intellectual Property?” 132.

⁵⁰⁰ *TracFone Wireless, Inc. v. Dixon*, 475 F. Supp. 2d 1236 (2007); see also Pamela Samuelson, “Freedom to Tinker” 20.

⁵⁰¹ *MIDY Industries, LLC. v. Blizzard Ent., Inc.*, 616 F. Supp. 2d 958 (2009).

⁵⁰² *Storage Technology v. Custom Hardware Engineering*, 421 F.3d 1307 (2005); *Lexmark v. Static Control Components*, 387 F.3d 522 (2004).

⁵⁰³ Pamela Samuelson, “Freedom to Tinker” 18-19; Electronic Frontier Foundation, “Unintended Consequences: Fifteen Years under the DMCA”; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 28; see for example Section 5.2.2.4 on the OV-chipcard hack.

⁵⁰⁴ Martin Scenfileben, “The Emerging EC Fair Use Doctrine” 533-534 (the Mulholland Drive case).

⁵⁰⁵ Pamela Samuelson, “Freedom to Tinker” 15 and 20.

⁵⁰⁶ Pamela Samuelson, “Freedom to Tinker” 21.

rised copying of digital works but also create techno-legal barriers that restrict wider access to and dissemination of knowledge”.⁵⁰⁷ The main issue that makers and hacktivists have with technological measures like DRM is that the law itself prevents them from “exercising their own right to respond to these techno-legal restrictions” because “the act of circumvention per se is rendered unlawful under international and state laws, regardless of whether the circumvention is carried out for a lawful use” such as for private and non-commercial copying.⁵⁰⁸ There is an imbalance and lack of fairness in the law because “copyright owners may, with some exceptions, protect the technological measures they employ to prevent access and copying, while users are not similarly free to defeat those measures”.⁵⁰⁹ The law as it currently stands gives too much control to owners and creators of information and technology to decide how the latter can be accessed or used. As Lessig and Cohen argue, hackers as well as ordinary users should have “a right to resist, or ‘hack’ trusted systems to the extent that they infringe on traditional fair use” or other limitations and exceptions to intellectual property rights.⁵¹⁰

The frustration that makers and hacktivists have with anti-circumvention rules is further exacerbated by the fact that in actuality these technological measures are never foolproof or completely “effective”, and it is quite trivial for hackers to get around or break them.⁵¹¹ However, despite the ease by which these measures can be defeated, hackers are dissuaded from hacking these measures because the law itself makes such circumvention illegal, regardless of the lack of

⁵⁰⁷ Michael Dizon, “Participatory democracy and information and communications technology” 15; see also Christophe Geiger, “The answer to the machine should not be the machine: safeguarding the private copy exception in the digital environment” 123; see also Lawrence Lessig, *Code: version 2.0* 175; Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 16.

⁵⁰⁸ Michael Dizon, “Participatory democracy and information and communications technology” 16; see also Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, arts 5(b) and 6(4) (but the exception is subject to “the absence of voluntary measures taken by rightsholders”).

⁵⁰⁹ Jane Ginsburg, “Copyright and Control Over New Technologies of Dissemination” 1634.

⁵¹⁰ Lawrence Lessig, *Code: version 2.0* 191-192; see also Julie Cohen, “A Right to Read Anonymously” 999-1000.

⁵¹¹ Christopher Soghoian, “Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them”; Graham Longford, “Pedagogies of Digital Citizenship and the Politics of Code” 83; Michael Dizon, “Participatory democracy and information and communications technology” 17-18; Lawrence Lessig, *Code: version 2.0* 179; Michael Dizon, “Does Technology Trump Intellectual Property?” 131-132;

malicious intent or purpose. In truth, based on my discussions with hackers, it is the very possibility or threat of prosecution rather than the actual filing of court cases that creates a chilling effect.⁵¹² For instance, the hackers I met recount how people they know stopped offering proxies to get around the block of The Pirate Bay in the Netherlands or providing Tor⁵¹³ services after receiving formal cease and desist letters from private companies or informal telephone calls and communications from public authorities. As a result, through the use of techno-legal controls, anti-circumvention rules doubly restrict what makers and hacktivists can do with information and technology and nullify their ability to perform all six common acts of hacking – explore, break, learn, create, share and secure. Furthermore, when access to and use of technology and intellectual property are so thoroughly locked down in this manner, a long list of hacker norms and values are stifled: openness, freedom of information, freedom of access, freedom of expression, individual autonomy and liberty, transparency, curiosity, creative and innovation, community development, and social development.⁵¹⁴

4.5 Conflicts and correspondences between hacking and law

Based on the foregoing normative and axiological analysis, existing technology laws and policies tend to restrict rather than support makers and hacktivists. In general, computer crime laws are very broad and restrictive and over-criminalize hacking. Because of the vague and low legal thresholds for committing computer security crimes, many hacking activities, including those that are creative or innocuous, are subject to criminal prosecution. While intellectual property laws are

⁵¹² See Electronic Frontier Foundation, “Unintended Consequences: Fifteen Years under the DMCA”.

⁵¹³ The Onion Router (Tor), <<https://www.torproject.org/>> accessed 28 July 2015 (a system that allows users to use and access the internet anonymously).

⁵¹⁴ See Michael Dizon, “Participatory democracy and information and communications technology” 18; see Christopher Kelty, “Geeks, Social Imaginaries, and Recursive Publics” 185; see Josh Lerner and Jean Tirole, “The Economics of Technology Sharing: Open Source and Beyond” 101.

meant to promote the creation and dissemination of creative works and inventions, there is an evident imbalance in these laws because they provide greater protection to the rights of creators and inventors at the expense of the rights of the public to reasonably use these creations. So while creators and inventors are granted extensive and exclusive rights of control over their creations, the corollary limitations and exceptions to these rights that could benefit hackers and ordinary users and preserve the intellectual property balance are few and far between. As discussed above, the situation is made even worse for makers and hacktivists because contracts and technological protection measures have been used to expand and ratchet up the application of computer crime and intellectual property laws.

The above examination reveals the numerous conflicts and incongruities as well as some fundamental correspondences and similarities between the goals and values of hacking and those of hacking-related laws. It is curious to see how hacking and the law share and seek to protect and promote essentially the same social values, interests and goals, yet in practice each has different and often opposing normative views and approaches as to which specific values to prioritize and how to achieve them. Computer crime laws have a laudable goal of safeguarding the integrity and security of information systems, but their restrictive approach (particularly the offense of illegal access) severely curtails what activities and projects hackers can reasonably and legally undertake. With regard to intellectual property laws, hackers are prodigious creators and users of information and technology but their ability to innovate is constrained by the quite limited exceptions to the free and open use or reuse of copyrighted works and patented inventions. On top of this, the controls and prohibitions under computer crime and intellectual property laws are further amplified and enlarged by the use of ever more restrictive contracts and anti-circumvention technologies and rules that tend to both legally and technically pre-

clude potentially creative and unexpected uses of protected information and technologies.

What is ironic though is that, despite all these, the above laws essentially share some of the same values of hacking. Like intellectual property laws, the main goal of hacking is to produce creative works and innovative technologies and disseminate them as widely as possible. Protecting the security of computer systems and data, which is the primary objective of computer crime laws, is considered an important value as well among the hackers I met. This means that, while they may have serious differences, hacking and law are connected on a fundamental level and, through these areas of connection and intersection, it may be possible to resolve the tensions between them.

Based on the above, it comes as no surprise then that hackers and the law are constantly interacting with one another, and why they seem determined to question and challenge each other's position. The clashes as well as congruence between makers and hacktivists and the law are thrown into greater relief in the next chapter, which examines how hackers actually view, respond to and interact with law and public authorities. Zeroing in on these plural and complex interactions is pivotal since they serve as the crucial means or mechanisms by and through which technology laws and policies concerning hacking are developed, contested, negotiated and remade.

CHAPTER FIVE

Hacking's interactions with law

This chapter delves into actual conflicts and interactions between makers and hacktivists and the law. Through interviews with hackers and observations at various hackerspaces and hacker events, the chapter presents makers' and hacktivists' perceptions and opinions about law and public authorities through their eyes and in their own words.¹ Furthermore, their different responses to law are examined. The chapter contains detailed cases and examples of how makers and hacktivists strive to ignore and avoid the law, change and resist it, or work within and use the legal system to achieve their techno-social goals.

5.1 Perceptions and attitudes of hackers toward law and authority

As seen in the preceding chapter, due to the conflicts as well as correspondences between hacker norms and values and the goals and priorities of technology laws and policies, the views and reactions of makers and hacktivists to law and public authorities are not only complex but also quite fraught.

¹ Note that some references to my interviews and conversations with hackers in this chapter are completely anonymized so as not to reveal their identities or make them identifiable.

5.1.1 PROBLEM WITH AUTHORITY

According to Levy, one of the tenets of hacker culture is to “mistrust authority”.² And as with other types of hackers, there is a strong distrust and even disdain of public authorities among the makers and hacktivists I observed and spoke to. Hackers tend to have a rebellious spirit or anti-establishment attitude, and they generally dislike hierarchies and other forms of centralized control or power. Hacktivist D observes, “mostly hackers don’t assume authority themselves or even reject authority”.³ This animosity towards authority pervades hackerspaces as well. As Maker C points out, “To me a hackerspace idea always has this anti-establishment type of feel. And that’s the difference for me. It has a kind of, there’s this rebelliousness”.⁴ Maker E also notes that it is possible to view hackerspaces and the maker movement as “being more like a movement against suppression”.⁵ Hackers’ aversion to authority can be reasonably traced to non-conformity, which is a constitutive part of hacking and hacker culture. As Maker I reflects, this is all “part of the non-conformist culture that is also a part of hacking”.⁶

Makers and hacktivists have varying ideological positions and political leanings. Some refer to themselves as anarchists or communists, others embrace libertarian ideals, many may be called liberals, and quite a number can be labeled as apolitical. However, because of the strong connection of the origin and development of the Dutch hacker scene with the squatter movement, their general orientation seems to veer or fall towards the left of the political spectrum. Hacktivist F confirms, “I would call it left. Radical, I don’t really like the word. Left, sort of the Dutch squatter scene”.⁷ While some hackers agree with libertarianism, they seem to approach it critically. As Hacktivist

² Steven Levy, *Hackers* 29.

³ Interview with Hacktivist D.

⁴ Interview with Maker C.

⁵ Interview with Maker E.

⁶ Interview with Maker I.

⁷ Interview with Hacktivist F.

B says, “I can empathize with the libertarian ideology there, although I think as good as libertarianism is in general, it neglects the social aspect of any exchange of goods”.⁸ Despite the melding of the anti-establishment spirit and the strong communitarian ethos in the hacker community, not many describe themselves as radicals, anarchists or communists, possibly due to the unwanted baggage that accompany those labels. Even Hactivist C who self-defines as an anarchist or communist says, “This new reality we should call it anarcho-communist. It sounds like something that is quite radical but it is totally common sense.... a kind of framework that is anarcho sort of communist without being dogmatic about it”.⁹

The acrimony that hackers, especially hactivists, feel about public authority is not based solely on ideological or political grounds but also their actual knowledge of and experiences dealing with government. Hactivist D states, “The problem with authority is that they, most often than not, place themselves above the law”.¹⁰ On top of that, many hackers believe that the government is technically incapable of tackling important issues relating to the governance of the networked information society. For instance, Hactivist B cites, “the blatant incompetence with which the state interacts in online affairs”.¹¹ From personal experience, Ethical Hacker A explains, “If you’re working in the government, the people are avoiding all kinds of risks, all kinds of responsibilities. They’re just not interested in improving the system”.¹² While the notion that states or governments “are dead”¹³ is not shared widely among hackers, many are of the view that hacking and authority are antithetical to each other. As Ethical Hacker A laconically explains, this is so because, when working in or with government, there is “no creativity, no innovation, no curiosity”, which are the main motivations

⁸ Interview with Hactivist B.

⁹ Interview with Hactivist C.

¹⁰ Interview with Hactivist D.

¹¹ Interview with Hactivist B.

¹² Interview with Ethical Hacker A.

¹³ Interview with Hactivist C.

and goals of hacking.¹⁴

As much as possible makers and hacktivists want to have nothing to do with centralized authorities. Hactivist C says, “I’m not going to talk to a politician to try to explain some point of what’s going on because it’s a waste of time... a dead end”.¹⁵ During my time with the hacker community, the underlying animosity and tense relationship between hackers and public authorities was quite palpable. Ethical Hacker A points out, “I don’t like the government guys, but the government guys also don’t like me”.¹⁶ Hactivist F is more direct, “From a moral perspective, they [the government] should just mind their own business”.¹⁷ For Hactivist D, “I don’t really deal very often with the government. They don’t get in my way for sure”.¹⁸ The conflict between hackers and public authorities can be attributed to a clash of cultures. According to Hactivist C, there is “no point in talking to politicians, there’s no point... because of all these politicians are there because of a mindset that is totally alien to what I’m going to tell them”.¹⁹ In general, hackers do not want to deal with the government, much less work for them. “No, I’m explicitly not working for a government organization at all”, exclaims Ethical Hacker A.²⁰ Hackers expressly avoid working in or for government “because governments tend to be soul-crushing operators and are not terribly fit and receptive to” hackers.²¹ Ethical Hacker A recounts, “In general in my experience, they’re not interested in improving. And if they’re not interested in improving, I’m not interested in that kind of job since it will be the same all over again”.²²

¹⁴ Interview with Ethical Hacker A.

¹⁵ Interview with Hactivist C.

¹⁶ Interview with Ethical Hacker A.

¹⁷ Interview with Hactivist F.

¹⁸ Interview with Hactivist D.

¹⁹ Interview with Hactivist C.

²⁰ Interview with Ethical Hacker A.

²¹ Interview with Maker H.

²² Interview with Ethical Hacker A.

5.1.2 TROUBLE WITH THE LAW

Hackers' acrimony toward public authorities also seems to be partly based on their perception that the authorities use the law to attempt to control and restrict their hacking projects and activities. The hackers I met consider laws and their restrictive applications as having negative effects and adverse impacts on their practices, norms and values. In relation to the perceived lack of fairness in the treatment and response of the law to hacking, makers and hacktivists hold the position that computer crime laws impose "disproportional penalty for" their activities.²⁴ According to a hacker, there are "now lots of punishment for, measures for hackers".²⁵ And this is made even worse by the government's attempt to impose stricter and harsher laws on hacking. A hacker relates how, "I'm really worried about the proposal that's now in place for" the revision of Dutch computer crime law.²⁶ Hackers are anxious because "the current proposals, which are by the way a harshening of rules for the computer crime law".²⁷ Many believe that "so far the moves are made to worsen... [an] already bad situation".²⁸ They are concerned that "becoming a suspect is very easy" under the proposed legislations.²⁹ Part of the proposed amendments is the grant of powers to the government to force people to disclose their encryption keys.³⁰ According to a hacker, the "mandatory giving of your crypto passwords, that really affects us" since encryption is necessary to preserve the security and privacy of people and their systems.³¹ "Having to hand over your decryption keys" is extremely problematic for hackers.³² For example, "because our servers run on encrypted

²³ Note that, due to the sensitive nature of the topics and information contained in this section, the references to my interviews and conversations with hackers are completely anonymized so as not to reveal their identities or make them identifiable.

²⁴ Interview.

²⁵ Interview.

²⁶ Interview.

²⁷ Interview.

²⁸ Interview.

²⁹ Interview.

³⁰ Interview.

³¹ Interview.

³² Interview.

hard disks and we want to be able to maintain the position where we can't be forced into giving other people's data".³³ It should be noted though that the proposed update to the Dutch computer crime laws on decryption orders is limited to the two specific cases of terrorism and child pornography.³⁴ It is worth noting that the Public Prosecution Service even "published a questionnaire on hacking and to ask the public how they should punish hacking".³⁵ This did not go over well with the hacker community and they published an open letter to the Public Prosecution Service contesting the categorization of hackers as criminals and hacking as a criminal activity.³⁶

For hackers, computer crime laws have also impeded computer security, which is not the exclusive domain of security researchers and ethical hackers, but is of paramount concern for all types of hackers. A hacker observes that the law is "affecting security research more and more, this particular subset of hacking".³⁷ According to the same hacker, while admittedly "the amount of, let's say, the number of real prosecution of researchers is still in the low end of the scale", the negative impact on security research is very real.³⁸ Bambauer and Day note that "[l]egal threats unquestionably influence researchers' actions, as they learn from prior controversies".³⁹ As the law currently stands, there are "quite a few loopholes that this hacker or other person has to jump through to not get prosecuted. It's still [a] fairly shady area".⁴⁰ A hacker relays how the law can inhibit the exploration and testing of computer systems: "If you're a web pen tester then if you want to say make sure some government or company's site is secure then you have way more issues".⁴¹ The hacker continues, "I do think about [it].

³³ Interview.

³⁴ F.W.J. van Geelkerken, "Proposal for the Dutch Computercrime Act III; A critique" 2.

³⁵ Interview.

³⁶ "Open brief aan OM: Hacken" <<http://www.randomdata.nl/blogs/node/85>> accessed 30 August 2014; "Open brief aan OM: Hacken" <<http://computervrede.nl/2014-08-26-OpenbaarMinisterie/>> accessed 30 August 2014.

³⁷ Interview.

³⁸ Interview.

³⁹ Derek Bambauer and Oliver Day, "The Hacker's Aegis" 34.

⁴⁰ Interview.

⁴¹ Interview.

Well, is this worth the risk? So if you crawl a website and the system overloads then they might try to get you convicted for a denial-of-service attack or something like that".⁴² For another hacker, "I can think of several projects or ideas that I never engaged in because the risks were simply too high and I couldn't be bothered".⁴³ As a result, when testing and securing systems or disclosing security vulnerabilities, "this is typically something that then people try, they either get lost or get such a hostile reception or whatever".⁴⁴ The makers and hacktivists I spoke to cite examples of security researchers being investigated, sued or criminally prosecuted.⁴⁵ A hacker relays how "things like the prosecution of Jeremy Hammond or Weevil" who were US hackers in United States were criminally prosecuted for engaging in acts of hacktivism and disclosing security vulnerabilities "could have happened here" in the Netherlands.⁴⁶ A hacker cautions that "at some point, people must realize that if you make your security research impossible, you get into the argument, if you outlaw guns only the criminals will have guns. But that is basically what we're slowing moving to actually".⁴⁷

Hackers believe that intellectual property laws too have a detrimental impact on hacking. A hacker explains how the restrictions imposed by copyright affect one's ability to innovate: "I cannot continue doing what I like doing. I think that's a negative flow of the whole creation process".⁴⁸ Another hacker concurs that intellectual property laws "most definitely influences what I do".⁴⁹ Hackers dislike the restrictive uses of intellectual property rights and laws. As one hacker states, "I think that many things show that it's [intellectual property] a hindrance because there's already a psychological effect".⁵⁰ Quite

⁴² Interview.

⁴³ Interview.

⁴⁴ Interview.

⁴⁵ Interviews.

⁴⁶ Interview; see also Cassandra Kirsch, "The Grey Hat Hacker" 386-387; see also Janet Reitman, "The Rise and Fall of Jeremy Hammond: Enemy of the State"; see also Hanni Fakhoury, "The U.S. Crackdown on Hackers Is Our New War on Drugs".

⁴⁷ Interview.

⁴⁸ Interview.

⁴⁹ Interview.

⁵⁰ Interview.

a number of hackers stopped working on their projects because of intellectual property concerns or issues.⁵¹ For instance, some desisted in incorporating advanced features in 3D printers because a commercial company owned the patents to the underlying technologies and they did not want to get sued. As one hacker contends, “I think in the end it’s very damaging for society as a whole if only like a small group of people in a top-down way decides what technology is built, when it’s built, at what price it’s sold, and how we’re all going to use it”.⁵² A hacker similarly believes that “the system that creates those laws is so far outside our democratic system as it is supposed to work because it’s basically now entirely privatized and 100% non-democratic”.⁵³ Many consider copyright laws to be outdated or “antiquated” and need to have “a big update”.⁵⁴ A hacker remarks, “I think... intellectual property, especially the way that intellectual property law is being used right now, that needs to change. I mean the hacking ethic is completely at odds there”.⁵⁵

Difficulties with intellectual property laws are particularly acute among makers. On the one hand, there is the constant fear or threat of being sued for copyright or patent infringement.⁵⁶ As one hacker advises, “if you would make a machine you have to check” whether the core technologies are patented and “you want to be very careful about [not] infringing” them.⁵⁷ Based on experience, a hacker explains how “the particular technology that I am using, it’s still covered by quite a few [patents], so you basically run into hot water”.⁵⁸ The hacker further states: “The company that developed the technology did such a good job of patenting such a broad range, so you can’t really get close without being quite similar” and thus infringe the patent.⁵⁹ Many believe

⁵¹ Interviews.

⁵² Interview.

⁵³ Interview.

⁵⁴ Interviews.

⁵⁵ Interview.

⁵⁶ Interviews.

⁵⁷ Interview.

⁵⁸ Interview.

⁵⁹ Interview.

the “patent system is kind of broken”.⁶⁰ A hacker laments the possibility that, “if we’re only allowed to create 3D printers that are fairly limited because someone has patented some mechanism, that really limits the powers of the hackers”.⁶¹ Another hacker is likewise concerned, “I definitely do not agree with the fact that right now a lot of companies are essentially getting extorted. ‘Hey look, we’re going to sue. That’s going to cost you \$20M. Yeah, pay up.’ I think that’s an abuse of the system”.⁶² On the other hand though, as a matter of principle, makers do not wish to apply for patents over their creations because this goes against their sharing ethos and the norms and values of openness and freedom of access.⁶³ But the fact remains that commercial companies file and obtain patents.⁶⁴ “Especially in 3D printing, you are seeing now some proliferation of new patenting”, explains one hacker, “Stratasys gets patents, now also MakerBot is getting patents”. There is a great apprehension among makers that it “starts becoming something where a lot of people are investing in patents which will not go away for 20 or more years. So we’re getting ourselves into a very hairy mess, I would say, if we don’t do anything against it”.⁶⁵

All in all, restrictive laws and policies tend to have a chilling effect on hacking and increase the levels of concern and anxiety among hackers.⁶⁶ The hackers that I met all agree that the law “definitely” and “very much so” influences what they do.⁶⁷ They are constrained by “computer crime laws” because “you can interpret them very broadly. Anything becomes a crime if you look at it from a certain point”.⁶⁸ Some are “scared that you could do something that is not allowed or might not be allowed”.⁶⁹ Others feel that “you lose all transparency

⁶¹ Interview.

⁶² Interview.

⁶³ Interview.

⁶⁴ Interview.

⁶⁵ Interview.

⁶⁶ Interviews.

⁶⁷ Interviews.

⁶⁸ Interview.

⁶⁹ Interview.

because transparency means getting called up” by the police.⁷⁰ And a few are “worried about... what happens in the shadows”.⁷¹ A hacker discloses how, “I try to fight not to get too paranoid, you know, about that”.⁷² Otherwise, “it institutes paranoia”.⁷³

5.1.3 LEGAL AND EXTRA-LEGAL MEANS⁷⁴

It was quite surprising to learn from some of the hackers that I spoke to that the commencement of formal criminal prosecutions or the filing of court cases is not the usual or preferred way by which public and private actors deal with what they consider problematic hacking technologies or activities. In truth, “a lot more happens via legal intimidation... than via actual prosecution”.⁷⁵ According to another hacker, the police “will first try extra-legal methods” from calling them up and informal warnings to veiled threats and intimidations.⁷⁶ The hacker continues, “I’ve seen many activist sites, a lot of the legal trouble you get into doesn’t actually follow law or legal procedures”.⁷⁷ A hacker also recounts, “By far, the most censorship I’ve seen has all been completely extra-judiciary, extra-legal. Simply informal requests of the police... or parties like that towards ISPs directly like, ‘Hey, can you take that down?’ ‘Oh sure, we’ll take that down’”.⁷⁸ A hacker explains how they “sometimes get cease and desist letters or phone calls” regarding websites or services that host potentially copyright-infringing or controversial content.⁷⁹ These informal requests to takedown websites “in my experience” happen “a lot more than the official channels through which these are done”.⁸⁰ Hackers who receive a letter or a so-

⁷⁰ Interview.

⁷¹ Interview.

⁷² Interview.

⁷³ Interview.

⁷⁴ Note that the references to my interviews and conversations with hackers are completely anonymized so as not to reveal their identities or make them identifiable.

⁷⁵ Interview.

⁷⁶ Interview.

⁷⁷ Interview.

⁷⁸ Interview.

⁷⁹ Interview.

⁸⁰ Interview.

called “lawyer gram” from the government or a private company, “tend to stop”.⁸¹

In addition, hackers are subjected to actual or veiled threats, intimidation or harassment from public authorities and private companies. “When I publish about politicians, I always have to be aware that I don’t make them angry”,⁸² explains a hacker. There can be “threats sometimes because in politics people get angry sometimes so they say they want to hit you or something”.⁸³ In relation to a court-mandated nationwide block by Dutch internet service providers of the peer-to-peer file sharing website, The Pirate Bay, some hackers sought to provide proxies and other technical means to circumvent the block, but the private companies involved sued “one person and they threatened a whole bunch of others”.⁸⁴ Most threats of legal action “never actually came to court” since many hackers desisted.⁸⁵ However, a hacker explains, “There’s one who didn’t [take down his proxy] and he’s still in a legal mess. They really got after him. Like he had his bank account closed, his Paypal account closed off. It’s nasty”.⁸⁶

In relation to Wikileaks and whistleblowers, the response of many governments has been quite extreme. A hacker relates how

Everyone who’s been seriously involved over at Wikileaks has actually been physically threatened basically by, not just the US government. There are other organizations and individuals. So we have a Canadian cabinet level adviser who says, on television, “Oh, I think we should just run bomb all these guys”.⁸⁷

“The most powerful military alliances on the planet are seri-

⁸¹ Interview.

⁸² Interview.

⁸³ Interview.

⁸⁴ Interview.

⁸⁵ Interview.

⁸⁶ Interview.

⁸⁷ Interview.

ously considering extra-judicially killing people and you know they have the means to do it. And you know they have the willingness to do it”, the hacker continues, “And so they’re actually considering doing that. So that’s also when several people got out of Wikileaks and said, ‘Look, you know, this is all fun and well, and you know, I’m not against a little risqué activism, but this is a little bit too much’”.⁸⁸ According to the same hacker, “even worse, they might just extrajudicially kill you. The fact that is even a serious part of a discussion for people who have done nothing else than just to report... [on] war crimes done by the very same government, by the way... you have a fair idea of how messed up we are as a society”.⁸⁹

Some makers and hacktivists also point to the Dutch government’s animosity towards and harassment of well-known journalist Brenno de Winter who hackers consider to be a member of their community and who sometimes acts as an intermediary between them and the government.⁹⁰ After he published how he was able to travel for free using a cracked OV-chipcard, de Winter was questioned as a suspect for four hours and investigated by the public prosecutor for months.⁹¹ A hacker notes how the government only investigated de Winter despite the fact that there “were a lot of other people of the big news agencies... who did it also and they didn’t get the police on their door”.⁹² While the public prosecutor ultimately decided not to file a case against de Winter on the ground of journalistic interest, de Winter still had to go through an arduous process and hire counsel during the period of investigation.⁹³ It is interesting to note how the hacker and internet communities raised €7,500 for de Winter’s legal defense.

⁸⁸ Interview.

⁸⁹ Interview.

⁹⁰ Interviews.

⁹¹ Sander van der Meijs, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <<http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart>> accessed 16 June 2015.

⁹² Interview.

⁹³ Sander van der Meijs, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <<http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart>> accessed 16 June 2015.

⁹⁴ But even after the investigation against him was dropped, hackers believe that de Winter continues to be scrutinized and hounded by the government. According to some hackers, de Winter is under surveillance by the government and that “he was followed” and the police “had a big dossier about” him.⁹⁵ Furthermore, it appears that “all police forces in the Netherlands have been notified of Brenno being a shady person that might be trying to enter government buildings with false or forged identity papers. His picture hangs in certain” places.⁹⁶ A hacker relates how de Winter “was visiting a certain ministry in The Hague and there were actually specific protocols to deal with him as a person when he was to enter the building”.⁹⁷

Many hackers feel that the actions taken by public authorities against them are unfair and disproportionate. For instance, a hacker recounts how “I heard... some hackers who hacked the school website, the team High Tech Crimes busts into their homes. Six people and some of them have complete gear with bullet-proof vests busts into the home of a school kid of 16 or 17 years old”.⁹⁸ With respect to the blocking of websites, a hacker is of the opinion that “if you then figure out that this website is illegal and you start blocking access to it and you censor it, that is a disproportionate move”.⁹⁹ Most hackers also balk at the attempts of public authorities to intrude or insinuate themselves into hacker events. For instance, “the Dutch High-Tech Crime Unit... wanted to have a presence at OHM”, an outdoor hacker conference.¹⁰⁰ A hacker relays how “We had like a long discussion about what are we going to do. We were violently opposing also the participation of the police in OHM, which they later withdrew luckily”.¹⁰¹

⁹⁴ Sander van der Meijs, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <<http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart>> accessed 16 June 2015.

⁹⁵ Interviews.

⁹⁶ Interview.

⁹⁷ Interview.

⁹⁸ Interview.

⁹⁹ Interview.

¹⁰⁰ Interview.

¹⁰¹ Interview.

5.1.4 PRESENCE RATHER THAN THE ABSENCE OF LAW

Despite their problems with law and authorities, the subject of law by itself is generally not top of mind or a priority concern among the makers and hacktivists I observed. Hackers do not usually spend their time thinking about or discussing the meanings, intricacies and nuances of law.¹⁰² They primarily focus on technical and social issues, and legal matters are not normally raised or discussed unless these become a significant concern or have a direct impact on the technical and the social dimensions of hacking. For instance, while there are talks on legal topics and issues at hacker camps, they are meager compared to the overwhelming number of technical presentations and workshops.¹⁰³ This is expected given that, echoing the view of many hackers, “Personally, my perspective of the world is not a legal one”.¹⁰⁴ Hactivist F captures how most hackers view the law: “My natural inclination to solve problems is not a legal solution. To me, it’s always if you need a lawyer probably something has gone wrong somewhere or at some point”.¹⁰⁵ Maker D goes even further and says that the goal is “to only have to know the law superficially” since “I just do the bigger picture” and other people like lawyers can take care of the specific legal issues.¹⁰⁶

Hackers’ general attitude towards law can be characterized as a mix of ambivalence and indifference. As discussed in greater detail below in the sections on hackers’ responses to law, the makers and hacktivists I spoke to prefer to ignore and avoid laws and legal issues, but, as a practical matter, they also see the law as the basis or source of fundamental rights and freedoms and they are willing to directly engage with laws and public authorities to achieve a social goal or

¹⁰² Interview with Hactivist B.

¹⁰³ See OHM2013, “Call for Participation”; see OHM2013, “Program”.

¹⁰⁴ Interview with Hactivist F.

¹⁰⁵ Interview with Hactivist F.

¹⁰⁶ Interview with Maker D.

to improve the law. Maker J speaks about the relationship between hacking and law: “I mean they’re not completely at odds but I see that there is conflict, yes”.¹⁰⁷ Maker E adds, “So yeah in certain aspects we want to have laws and regulations, and in others we go like, ‘Hey don’t limit me, I want to be free’”.¹⁰⁸ This ambivalence towards law is further exacerbated by a common belief among hackers that law is slow-moving and outpaced by technological change: “If you look at law, rules and regulations have always trailed behind innovation”.¹⁰⁹ Maker E continues, “since the industrial revolution innovation is going so much faster.... the gap between innovation and lawmaking grows every year too, if you ask me”.¹¹⁰

Despite their initial indifference and ambivalence toward law, hackers still see the importance of having laws and the necessity of dealing with legal and policies issues that affect hacking. Even though most hackers bear a strong animosity against public authorities, their outlook and approach to law in contrast is less antagonistic and can even be described as positive and constructive. So, while many makers and hacktivists can imagine or strive for a world without hierarchies and centralized authorities, they have no wish to achieve a state of “anomie” since they recognize the need to have laws and other rules of behaviors to govern individual and social conduct.¹¹¹ They consider law to be an integral part of society. As Maker H explains, “I consider law as part of the social complex that [we] are in”.¹¹² For Maker J, there is no reason for getting rid of law altogether since “I think we have to have something”.¹¹³ Asked about their opinions about law, Maker J states, “I mean it has room for improvement, but I think it’s good that it’s there”.¹¹⁴ Discussing the possibility of having less or more laws that

¹⁰⁷ Interview with Maker J.

¹⁰⁸ Interview with Maker E.

¹⁰⁹ Interview with Maker E.

¹¹⁰ Interview with Maker E.

¹¹¹ See Bruce Dohrenwend, “Egoism, Altruism, Anomie, and Fatalism: A Conceptual Analysis of Durkheim’s Types”

¹¹² Interview with Maker H.

¹¹³ Interview with Maker J.

¹¹⁴ Interview with Maker J.

apply to hacking, Maker J says, “The things we have right now is not, it’s not so bad that I would say that we’re better off without them”.¹¹⁵ Maker L believes that “there should be less laws. I think there should be basic laws”.¹¹⁶ Hactivist B concurs, “I say less probably... less would mean a lot less”.¹¹⁷ Others hold the view that “especially for a lot of these cases where we’re talking about hacking, there’s not really [any] law about it”.¹¹⁸ But Hactivist D believes, “I don’t think you can. Law is not like water, you can have more or less.... Better, you know, not more or less but better. Better laws so they’re more broadly defined or something”.¹¹⁹ Hactivist D continues, “I don’t need less of that. I need more of those kind of good laws”.¹²⁰

5.1.5 KNOW THE LAW MORE

Hackers’ knowledge of law varies greatly among individuals and groups. Their legal understanding can range from nil, basic or general to even substantial and specialized. Like many hackers I met, Maker G is quick to point out that “I’m not really a legal expert”.¹²¹ Maker A confesses, “I really don’t know a lot about it [law]”,¹²² while Maker E admits that in their hackerspace, “the knowledge about it [law] is very little.... To be honest, I don’t know much about those legal rules for pen testing” and computer crime laws.¹²³ In relation to intellectual property law, Maker K says, “a lot of young kids don’t even know what a patent is and what it really means”.¹²⁴ Maker H observes that hackers’ knowledge of law “varies from person to person. By and large their idea of what [one] can or can’t do is not entirely based in reality”.¹²⁵

¹¹⁵ Interview with Maker J.

¹¹⁶ Interview with Maker L.

¹¹⁷ Interview with Hactivist B.

¹¹⁸ Interview with Maker J.

¹¹⁹ Interview with Hactivist D (emphasis added).

¹²⁰ Interview with Hactivist D.

¹²¹ Interview with Maker G.

¹²² Interview with Maker A.

¹²³ Interview with Maker E.

¹²⁴ Interview with Maker K.

¹²⁵ Interview with Maker H.

This is compounded by the fact that some hackers do not know where to find legal information. “I think there’s also very little to be found on it [law]”, relates Maker E, “I wouldn’t know where to find any of that, if it already exists”.¹²⁶

But, like the FOSS developers who have become quite well versed in the substance and intricacies of intellectual property and licensing issues,¹²⁷ there are some makers and hacktivists who are familiar with specific or specialized areas of law. For instance, Maker J states, “I’m very aware of the law in these fields... both in the privacy law and security law”.¹²⁸ Unlike other hackerspaces, Maker L says, a “lot of people in the space... know about computer laws, know quite a lot about that or know how to find it”.¹²⁹ Maker C also says that intellectual property “is something everyone is cognizant about” in their hackerspace.¹³⁰ Based on my dealings with makers and hacktivists, while there are indeed hackers who are well informed about specific areas of law such as copyright and data protection, their legal knowledge is close to but still not on the same level as a general practice lawyer.

Whether they know a little or a lot about the law, the hackers I conversed with were fairly open and willing to learn more especially those rules and regulations that affected them. Maker L says, “most of the time I have general information that I read about. But if it really affects me... yeah I look up a law book and read about it that way”.¹³¹ For most hackers, the path to legal knowledge is mainly through self-study and a bit of learning and guidance from others. According to Maker D, “I read [the law] by myself.... I always do the research by myself”.¹³² For Maker L as well, “Yeah, I read the law sometimes, on

¹²⁶ Interview with Maker E.

¹²⁷ Gabriella Coleman, “Code is Speech” 425-426.

¹²⁸ Interview with Maker J.

¹²⁹ Interview with Maker L.

¹³⁰ Interview with Maker C.

¹³¹ Interview with Maker L.

¹³² Interview with Maker D.

certain parts, how things work. I find it interesting the law”.¹³³ Maker J explains the process further, “and then once I get some kind of grasp of that area, then I try to read more, learn more”.¹³⁴ For Hactivist E, “I read the actual laws, related parliamentary papers. I used the website of the Dutch Data Protection Authority, bought books, visited seminars, talked to various lawyers and legal academics”.¹³⁵ While some hackers actually read pertinent laws and court decisions,¹³⁶ others try to keep abreast of legal developments from online sources. For example, Maker L reads the blog of an IT lawyer who “everyday he posts about law issues related to IT, computer, web shops and those kinds of things, privacy.... yeah that gives a lot of information”.¹³⁷ To learn about cybercrime laws, Hactivist E reads the blogs of IT law scholars.¹³⁸

Studying the law on one’s own is not without difficulty. Some laws like the freedom of information regulations are “very hard to read, to understand and to grasp”.¹³⁹ While some found that “it was pretty hard”¹⁴⁰ to understand the law, others felt that “most of the law is also pretty straightforward. I don’t find it hard to read”.¹⁴¹ “Sometimes I just get the law book on the internet and read the law... how does it work, and it’s readable”, narrates Maker L, “Yeah sometimes it’s hard to understand, but sometimes you get the information from it [on] how it works”.¹⁴² Hactivist D explains how, for ordinary people, law should be easier to understand compared to computer programming since the “law as far as I’m concerned is in my language. Computer language is a different language that I still have to learn”.¹⁴³ This is one of the

¹³³ Interview with Maker L.

¹³⁴ Interview with Maker J.

¹³⁵ Interview with Hactivist E.

¹³⁶ Interview with Hactivist D.

¹³⁷ Interview with Maker L.

¹³⁸ Interview with Hactivist E.

¹³⁹ Interview.

¹⁴⁰ Interview.

¹⁴¹ Interview.

¹⁴² Interview with Maker L.

¹⁴³ Interview with Hactivist D.

reasons why hackers consider it their social responsibility to make technology more open, available and transparent for the general public, because, unlike normal people, they are much more comfortable and adept in the language of computers than the language of law.

Despite their ambivalence towards law, makers and hacktivists still grasp the advantages of knowing more about the law. In the same way they approach technology, hackers view the law as basically a system of rules and processes that they can understand and then use, subvert or remake (in other words hack). According to Maker H, some hackers consider the law “as another system that has its own loopholes and unforeseen consequences”.¹⁴⁴ For many hackers, learning about the law is both a practical and a tactical exercise. From a political or ideological point of view, Maker E argues, “you need to know what the law is in order to rebel against it”.¹⁴⁵ According to Hactivist B, it makes sense “to know when you are or aren’t breaking the law”.¹⁴⁶ As Maker E also explains, “you need to know what is acceptable and what is not in the eye of other people that are controlling you whether it’s a government or a police force or a military, you name it”.¹⁴⁷ Maker D recognizes the importance of the fact that “when I am politically active... I also have to understand the law”.¹⁴⁸ In their day-to-day lives, knowing the law is also a practical necessity.¹⁴⁹ As Ethical Hacker A says, “I’m interested in why it works, the way it works. From the professional point of view, for myself ... it’s really, really important, critically important” to know the law.¹⁵⁰ Similarly, Maker L recounts how for “my work, some things with my job, I do look up the law book for that. What the rules were and how the policy works so you know what you’re doing”.¹⁵¹ “So for me... it’s just very important... to make sure

¹⁴⁴ Interview with Maker H.

¹⁴⁵ Interview with Maker E.

¹⁴⁶ Interview with Hactivist B.

¹⁴⁷ Interview with Maker E.

¹⁴⁸ Interview with Maker D.

¹⁴⁹ Interview with Ethical Hacker A.

¹⁵⁰ Interview with Ethical Hacker A.

¹⁵¹ Interview with Maker L.

that I'm on the right side of the line", Ethical Hacker A explains, "so I think I need to be prepared as well for those kind of circumstances" where the law is involved.¹⁵²

5.1.6 GREATER ACCESS TO LAW AND LEGAL ASSISTANCE

What was really surprising about my conversations with makers and hacktivists is that, while they show a general ambivalence or indifference to law, they still recognize the value of knowing their rights under the law (especially fundamental rights such as freedom of expression, liberty and privacy) and having access to legal assistance, aid or advice in order to protect or uphold these rights. Hackers I spoke to agree that they need more help from lawyers since they often do not know what the limits of the law are. Maker E remarks, "It would be nice to at least be able to find out what the law would be or is, or if there are even laws to cover something like that".¹⁵³ According to Hacktivist B, lawyers can "at least raise awareness of what your rights are".¹⁵⁴ Hackers mainly get informal legal advice from acquaintances or friends who are lawyers or legal professionals. For instance, "being friends with [people with a legal background] helps in getting an understanding [of law]".¹⁵⁵ Maker K agrees, "Yeah I've been lucky. I've met quite a few good people along the way" who know the law.¹⁵⁶ When dealing with potential legal issues, "I got my IP lawyer to check it out.... He's a friend who's a patent lawyer. That's handy".¹⁵⁷

Only a few hackers though have this kind or level of access to law and legal assistance. As with most hackers who do not have convenient or immediate access to a lawyer, Maker L relates "But no, [I]

¹⁵² Interview with Ethical Hacker A.

¹⁵³ Interview with Maker E.

¹⁵⁴ Interview with Hacktivist B.

¹⁵⁵ Interview with Hacktivist B.

¹⁵⁶ Interview with Maker K.

¹⁵⁷ Interview with Maker K.

don't have my own lawyer or something like that".¹⁵⁸ Hactivist B further explains that while there are a few lawyers who can make themselves available to hackers, they are mostly "not pro bono".¹⁵⁹ Furthermore, digital rights organizations in the Netherlands do not "really provide that kind of support in the way, say the EFF does, assisting with court cases".¹⁶⁰ The current situation severely restricts the ability of makers and hactivists to receive sufficient legal protection or to properly enforce their rights. Maker D believes that "not having people that help you with the law" is a significant issue.¹⁶¹ "That's a major problem I think as well", states Hactivist B on the general lack of access of the hacker community to lawyers or legal assistance. As a result, many makers and hactivists end up undertaking hacking projects and activities that push the boundaries of technology and law with "no legal advisement of lawyers".¹⁶² Many hackers that I spoke to believe that having access to lawyers would be extremely helpful for them.¹⁶³

Even though makers and hactivists see the benefits of having access to a lawyer and there are a handful of legal professionals who are active in or have close ties to the Dutch hacker community, Maker H opines, "I wouldn't consider the lack of lawyers to be the most pressing diversity issue in that scene".¹⁶⁴ Despite the common desire to have more legal assistance, Maker H cautions that, "I wouldn't say you should go to a hackerspace if you are an IT lawyer or a lawyer in general" unless one is interested as well in working hands-on with technical projects.¹⁶⁵ In addition, hackers can be quite critical of lawyers specifically with regard to their lack of technical knowledge or understanding. Ethical Hacker A relates the problem with dealing with lawyers, "There are legal folks having some kind of discussion with me that's com-

¹⁵⁸ Interview with Maker L.

¹⁵⁹ Interview with Hactivist B.

¹⁶⁰ Interview with Hactivist B.

¹⁶¹ Interview with Maker D.

¹⁶² Interview with Ethical Hacker A.

¹⁶³ Interviews.

¹⁶⁴ Interview with Maker H.

¹⁶⁵ Interview with Maker H.

pletely out of this world, about possible risks, commas, punctuations and that kind of stuff” that are not relevant to technical issues.¹⁶⁶ A hacker recounts similarly disappointing experiences with lawyers when making a security report or disclosure: “Because it goes to the law firm and [they don’t] even... know what it’s about. They just say, OK we start looking at, you know, similar cases. Oh there was someone who actually broke into a bank, oh maybe it’s comparable”.¹⁶⁷ The hacker further recounts how legal departments in large companies do not understand the technology and “also make some stupid comments and annoying stuff”.¹⁶⁸ So, while hackers prefer to have better access to law and legal professionals, they are still very much averse to having to deal with government or company lawyers in adversarial proceedings or contentious contexts.

5.2 Hackers’ responses to law

In light of the above, members of the Dutch hacker community seem to perceive and approach the law in two distinct and opposing ways: first, as restrictive, unjust or outdated prescriptions made by centralized authorities that must be opposed or contested; and, second, as the basis or source of fundamental rights and freedoms that need to be protected or upheld. This dual outlook frames and informs how they respond to technology laws and policies. As Maker G remarks, it “depends per law what [their] action should be”.¹⁶⁹ Hackers’ general responses to law are: to ignore and avoid it; if it becomes impossible to keep the law away, to change or resist it; and, if it benefits the hacker community and society as a whole, to possibly work with, use or adapt the law. It is worth noting that hackers are rarely inclined to obey or conform to laws of the restrictive kind that they believe to be undemo-

¹⁶⁶ Interview with Ethical Hacker A.

¹⁶⁷ Interview.

¹⁶⁸ Interview.

¹⁶⁹ Interview with Maker G.

cratic or unjust.

5.2.1 IGNORE AND AVOID

Based on my observations of and interviews with makers and hacktivists, their natural tendency and default response is to ignore or avoid the law, especially those laws that they view as unduly restricting or controlling their rights and freedoms. This response springs directly from the hacker norms and values like individual autonomy and liberty and their general indifference and ambivalence to law. “I’m not a big fan [of the law] to put it mildly”, explains Hactivist B, “I generally don’t really concern myself that much with law”.¹⁷⁰ Likewise, Hactivist C says, “Basically in terms of law, to me, yeah it’s always been a piece of paper.... To me it’s never been a tool that I even considered as being relevant”.¹⁷¹ For some hackers, the reasons for ignoring or avoiding the law can be ideological or political. Hactivist C believes that “law has always been on the side of the people who wrote laws.... This sort of code of conduct, the code of law or this codex or set of principles is easily swept aside by those in power when they deem it necessary”.¹⁷² For Hactivist B, “they’re [laws] a nuisance and I have to know and deal with them”.¹⁷³

For others, ignoring or avoiding the law and public authorities is necessary to protect or promote the norms and values of curiosity and creativity and innovation. As Maker A says, “I really don’t want to think about it [laws and legal issues] when I’m creating something.... Just don’t think about it because that just stops the creative process”.¹⁷⁴ Hactivist C concurs, “To me the very notion of the law as it is inscribed is part of a system that always will shut these types of innovation out”.¹⁷⁵ Maker E recounts how publicly funded organizations

¹⁷⁰ Interview with Hactivist B.

¹⁷¹ Interview with Hactivist C.

¹⁷² Interview with Hactivist C.

¹⁷³ Interview with Hactivist B.

¹⁷⁴ Interview with Maker A.

¹⁷⁵ Interview with Hactivist C.

and projects “are the people that are really worried about lawmaking, thinking about it and talking about it. It’s not the ones that are innovative that are thinking about law, I think”.¹⁷⁶ Some hackers view the law as a distraction. Maker H relates how some hackers believe “you can only waste your time with [laws] and should best be ignored”.¹⁷⁷ Maker E says that in their hackerspace, “most people think that legalese and financial stuff is boring”.¹⁷⁸ “Now we’re not really putting a lot of time and effort on that [legal issues or concerns] here”, explains Maker E.¹⁷⁹ Maker A affirms, “Do I want to know more about it [law]? No, I don’t think so”.¹⁸⁰

Makers and hacktivists are aware that ignoring or avoiding the law can lead to breaking the law. But, on the whole, that does not stop them from engaging in hacking projects and activities. For example, the existence of patents over certain 3D printing technologies should normally prevent or stop people from hacking or building on these patented technologies without the inventor’s permission. But despite these patents, a hacker argues that, “For individuals and for groups, for social groups, I think it makes sense that people hack regardless of a patent or possibly even because of a patent”.¹⁸¹ The hacker further explains, “doing something that might be patented, it’s also, I would say, part of the non-conformist culture that is also a part of hacking”.¹⁸² For others, ignoring and breaking the law has a political or moral dimension. Hactivist A explains, “For me, copyright law now is a zone of law where the law is so broken and the system that makes the law is so broken that actually the morally right thing to do as a citizen of a democratic country is to essentially ignore it and make your own judgments”.¹⁸³ Maker I reflects on the connection between hacking and

¹⁷⁶ Interview with Maker E.

¹⁷⁷ Interview with Maker H.

¹⁷⁸ Interview with Maker E.

¹⁷⁹ Interview with Maker E.

¹⁸⁰ Interview with Maker A.

¹⁸¹ Interview.

¹⁸² Interview.

¹⁸³ Interview with Hactivist A.

breaking the law: “There’s a paradox there. Because hacking is doing something that is not as intended. Then breaking the law and hacking are also to some extent or, at least, kicking the boundaries, for example, changing something which voids the warranty”.¹⁸⁴ “We’re often, of course, skating along the edges of the law with so many things that we get up to”, points out Hactivist A, but “that doesn’t mean that I break everything all the time”.¹⁸⁵ Hactivist A continues, “But it does mean that I am now making my own moral judgments. Whereas in many other cases in my life, I defer to the law. I say, ‘Look, you know, we agreed that we’re going to do this. You know, we agreed in this country that we’re going to drive in a fashion, no more than 120’”.¹⁸⁶ For Hactivist B, there’s a tactical motive behind ignoring and avoiding the law: it’s “not so much because you shouldn’t break the law but at least have yourself covered and don’t get caught”.¹⁸⁷ Maker E adds, while they want to avoid the law, but still “you need to know what’s going on”.¹⁸⁸ But skirting rules and voiding warranties are things hackers are generally not worried about. Maker A remarks, “I know that if you open it up you void your warranty. Yeah, but I’m not really someone that brings something back that I broke”.¹⁸⁹ “As a consumer I just open it and I don’t claim warranty”, says Maker G.¹⁹⁰

¹⁸⁴ Interview with Maker I.

¹⁸⁵ Interview with Hactivist A.

¹⁸⁶ Interview with Hactivist A.

¹⁸⁷ Interview with Hactivist B.

¹⁸⁸ Interview with Maker E.

¹⁸⁹ Interview with Maker A.

¹⁹⁰ Interview with Maker G.

5.2.2 CHANGE AND RESIST

5.2.2.1 Legal change through hacking

There are many cases and contexts where it is not possible for makers and hackers to simply ignore or avoid the law. Whenever it has become unfeasible or impractical to steer clear or to “route around” laws and other restrictions,¹⁹¹ hackers’ customary reactions are to resist or to change them. These forms of responses are expected given the rebellious, anti-establishment and non-conformist attitudes that run in the hacker community. Furthermore, makers and hackers regard these restrictive laws as threats to their hacking practices, norms and values that must be contested and opposed. As Maker G says, “If you don’t like a law you should, I guess, strategically try to fix” it.¹⁹² “We need to fight many battles on many different fronts at the same time”, relates Hactivist F, “You need to fight technical battles, legal battles. You need to make sure encryption is still allowed in the future”.¹⁹³

There are a number of technological, legal or social ways by which makers and hackers change or resist laws, but their seemingly preferred method is quite understandably technical – to change the law through hacking. This is clearly evident in the cases of the campaign against electronic voting computers, Leaktober and the OV-chip-card hacks, which are discussed in the succeeding sections. Hactivist D explains how hacking can be useful with regard to changing restrictive or problematic laws: “Sometimes you just got to piss people off, you know. It shows where the problems, where the cracks lie”.¹⁹⁴ Hacking therefore becomes a way to raise awareness about and directly engage with legal issues and problems. “So you get that kind of discussions. And the only way to prove that you are right is showing that it’s

¹⁹² Interview with Maker G.

¹⁹³ Interview with Hactivist F.

¹⁹⁴ Interview with Hactivist D.

actually hackable, or you can compromise it or you can manipulate it or whatsoever”, claims Ethical Hacker A.¹⁹⁵

Several hackers I met are not hesitant about resisting the law and the threat of public sanctions. While makers are generally more concerned about the possibility of being sued for their hacking projects, hacktivists are not as fretful. “There’s no reason to be afraid of anything”, says Hactivist C, “one thing they have is this jail that you maybe then have to sit for a year, so what”.¹⁹⁶ A hacker explains how “when I was a teenager, I wasn’t repelled by computer crime laws”.¹⁹⁷ Other hackers view their resistance to law as a legitimate form of civil disobedience. “For some laws there can be civil disobedience”, states Maker G.¹⁹⁸ For Maker L as well, “Civil disobedience... a nice way of showing people, yeah, you can show me what you want but bad luck” since it will be opposed anyway.¹⁹⁹ For instance, after the Snowden revelations, the response of members of the Dutch hacker community was to resist and counteract mass government surveillance by developing, using and promoting the use of encryption and other privacy-enhancing software like Tor, OTR and Tails.²⁰⁰ While the aim of these actions is not to directly change the law, they seek to counter or neutralize the negative effects of mass surveillance and thus render such government policy ineffectual or irrelevant. A hacker recounts what transpired: “Fallout of what Snowden has done. People reacting to that, trying to build new tools, forming new alliances, people getting to know each other and having more politically motivated discussions, might be threatening to the interests of the state”.²⁰¹ Maker B believes that it’s good “to be extreme sometimes to make people aware of

¹⁹⁵ Interview with Ethical Hacker A.

¹⁹⁶ Interview with Hactivist C.

¹⁹⁷ Interview.

¹⁹⁸ Interview with Maker G.

¹⁹⁹ Interview with Maker L.

²⁰⁰ Tor Project <<https://www.torproject.org/>> accessed on 1 December 2015; Off-the-Record Messaging <<https://otr.cypherpunks.ca/>> accessed on 1 December 2015; Tails <<https://tails.boum.org/>> accessed on 1 December 2015.

²⁰¹ Interview.

things”.²⁰² Similarly, for Hactivist, F, “you need to do things that are a bit more, yeah, radical or campaign-like for people to get a feeling that you’re working on it” and making a difference.²⁰³ Hactivist A similarly reflects,

I actually now consider it a very good metric of [how] effective activism is if you feel the pressure. So if you’re not feeling anything, you know, if there’s no [pressure], then actually there’s no indication that you’re achieving anything as an activist, right? Because if nobody’s pushing back, then maybe they didn’t even notice you yet. And if they didn’t notice you as an activist, then obviously you need to try harder, right? Then you didn’t do your job.²⁰⁴

Hackers believe that hacking can produce legal change when needed.²⁰⁵ In response to the question of whether hacking can change the law, Hactivist B sardonically remarks, “It obviously does because we wouldn’t have computer crime law”.²⁰⁶

5.2.2.2 Hacking electronic voting computers

One of the most well known and much discussed cases in the Netherlands of hackers resisting and changing the law through hacking involves the campaign against electronic voting. In 2006, a few months before the general elections, a non-profit group that called itself “We don’t trust voting computers” launched a campaign to challenge the use of electronic voting machines in the country.²⁰⁷ The group included and was led by hackers, including Rop Gonggrijp, a prominent member of the Dutch hacker scene.²⁰⁸ The group was able to get their hands on a few voting machines to study and analyze by

²⁰² Interview with Maker B.

²⁰³ Interview with Hactivist F.

²⁰⁴ Interview with Hactivist A.

²⁰⁵ Interview with Maker H.

²⁰⁶ Interview with Hactivist B.

²⁰⁷ Rop Gonggrijp and Willem-Jan Hengeveld, “Studying the Nedap/Groenendaal ES3B voting computer” 2; see also “We don’t trust voting computers” <<http://wijvertrouwenstemcomputersniet.nl/English>> accessed 12 June 2015; see also Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 11; see also Leontine Loeber, “E-Voting in the Netherlands” 24.

²⁰⁸ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 11; see also Rop Gonggrijp and Willem-Jan Hengeveld, “Studying the Nedap/Groenendaal ES3B voting computer” 16; see also Leontine Loeber, “E-Voting in the Netherlands” 24.

way of a loan and purchases from two municipalities.²⁰⁹

In order to understand how the voting machines work and to test their security, the group thoroughly hacked the machines. They systematically took apart and analyzed the machines' physical hardware and components.²¹⁰ They reverse-engineered the software and reprogrammed the machines to play chess and to purposely miscount votes.²¹¹ The group easily discovered that the password to access the critical software "maintenance mode" was "'GEHEIM', the Dutch word for 'SECRET'".²¹² They also showed that the mechanical locks on all of the voting machines could be opened with the same physical master key, and spare keys could be ordered online by anyone "without any problem" for two Euros each.²¹³ In addition, the locks were trivial to pick.²¹⁴ Finally, they group demonstrated how the displays of the machines produced radio emissions that could be captured and reproduced by people outside of the polling place to reveal how a person voted.²¹⁵ It was this last vulnerability that proved to be the main undoing of the voting machines since it affected the secrecy of the ballot, which is an essential requirement of free elections.²¹⁶ Despite repeated attempts, the machines' vulnerability to the so-called "Tempest attack" (also known as "Van Eck phreaking" which is named after a Dutch security researcher) (see Section 4.2.4.1) that compromised voting secrecy could not be adequately fixed.²¹⁷

As a result of the hacking of the voting machines by the group,

²⁰⁹ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 2 and 16; see also see also Leontine Loeber, "E-Voting in the Netherlands" 24; see also Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 11.

²¹⁰ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 4-6; see also Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 11.

²¹¹ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 6-8; Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 5; see also see also Leontine Loeber, "E-Voting in the Netherlands" 24.

²¹² Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 4.

²¹³ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 3.

²¹⁴ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 3.

²¹⁵ Rop Gonggrijp and Willem-Jan Hengeveld, "Studying the Nedap/Groenendaal ES3B voting computer" 10-12; see also Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 5, 11 and 12.

²¹⁶ Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 12; see also Leontine Loeber, "E-Voting in the Netherlands" 24.

²¹⁷ Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands" 11 and 12.

coupled with their active campaigning, freedom of information requests, and threatening and taking legal action, the Dutch government ultimately changed the law on electronic voting, withdrew the regulation for certifying electronic voting machines, and suspended the use of electronic voting in the country.²¹⁸ Jacobs and Pieters, who are academic security researchers, reflect on the triumph of the campaign:

Looking back one must acknowledge that the pressure group has been incredibly effective and has reached its goals in a remarkably short time. It relied on a clear vision, technical skills, bravery, effective use of freedom of information rights, professional communication via their own newsletter and a very informative webpage, frequent and convincing media appearances, and, in the end, threats of legal actions. No politician (or civil servant) likes to have such an adversary.²¹⁹

“There was a large group of people... who were helping them and advising them and, you know, writing blog posts and talking to journalists and all that stuff”, narrates Hactivist A.²²⁰ Maker B also recounts, “there was public awareness, and the media started to talk about it, and then they could not do anything else than stop it”.²²¹ A hacker believes that “the most important aspect of [the campaign] was to get the media’s attention. Because if you cannot physically demonstrate a fault then there’s no story, and you need a story. Otherwise nothing happens in the Netherlands politically, right? If it’s not on television, it didn’t happen”.²²² Thus, by 2008, “the Netherlands returned to paper voting, with manual counting of the ballots”.²²³ According to Hactivist F, the campaign against voting computers “basically killed the whole electronic voting in the Netherlands. Up until now we still vote with pencil”.²²⁴

²¹⁸ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 11, 12 and 13; see also Leontine Loeber, “E-Voting in the Netherlands” 24, 25 and 26.

²¹⁹ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 14.

²²⁰ Interview with Hactivist A.

²²¹ Interview with Maker B.

²²² Interview.

²²³ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 2 and 14; see also Leontine Loeber, “E-Voting in the Netherlands” 26.

²²⁴ Interview with Hactivist F.

The makers and hackers I met fully subscribe to the aims and methods of the campaign against electronic voting and they deem it a great success and a fine example of how hacking influences the law.²²⁵ They unanimously “agree with those involved in hacking electronic voting computers”.²²⁶ Maker G considers it “a nice strategic achievement”,²²⁷ while Hactivist B describes it as “a nice campaign”.²²⁸ Maker L statement reveals the sense of pride and elation that hackers feel about the campaign: “I think it was great thing. I was a bit younger then and didn’t know much about it.... I would like to have been in the middle of it if it would be possible”.²²⁹

Aside from being able to change the law, the other reasons why the campaign is such a touchstone for Dutch hackers is that it required technical mastery to carry out, it involved the commons acts of hacking (most especially break, learn and secure), and it directly related to the norm and value of security. Maker L explains, “Yeah that was great. That was a great way to show people what was wrong with voting computers, and let people understand why they are a bad thing”.²³⁰ Maker D adds, “It was good to see how it could be faked. It was good to see how the government had a romantic view of ICT, and it wasn’t reality”.²³¹ The hackers I spoke to were particularly fond of how hacking itself played a key role in the campaign. “I like the hacking part”, explains Ethical Hacker A, “since in many cases, and this was a very good one in my opinion, it’s the only way to show that it’s really a problem in the real world”.²³² According to Ethical Hacker B, “I mean it’s good to look at it because there was a lot of wrong with it”.²³³ Through hacking, the campaigners were able to show what were the real risks and threats posed by the use of electronic voting machines

²²⁵ Interview with Maker B; Interview with Maker I; Interview with Hactivist F; Interview with Ethical Hacker A.

²²⁶ Interview with Hactivist E.

²²⁷ Interview with Maker G.

²²⁸ Interview with Hactivist B.

²²⁹ Interview with Maker L.

²³⁰ Interview with Maker L.

²³¹ Interview with Maker D.

and why the process that people used to exercise their right to vote had to change.

The hackers I spoke to emphasize the technical aspects of the campaign and the wide disparity between the technological knowledge and skills possessed by the campaigners versus those in government. “Almost everybody involved in computer science thinks that this is a bad idea. I feel that it’s a very bad idea”, explains Maker J, “It’s so unbelievable that the people who are very knowledgeable about the security of and how these kinds of voting computers work, that they are so against it”.²³⁴ According to Hactivist D, “you should be very cautious when basically the people who know most about computers in our society are saying this is a bad idea”.²³⁵ Maker E describes how the campaigners were like “scientists that basically told government like, ‘Hey we’re playing with very dangerous toys here, and you need to change your policies’”.²³⁶ While it is easy to be enamored with technology, the voting computers campaign illustrates the importance of always having a critical view or stance in relation to technology. As Hactivist E points out, “We need to apply critical thinking everywhere we introduce computers”.²³⁷ Maker J explains further, “This is also something that I see very often. They think, well, we can improve this process by using computers. But I think, well, I know about these things and then, often you start thinking about the implicit things that are there in the analog process” that actually make it better and more secure.²³⁸ According to Maker D, hackers “helped to change that, to show that their [the government’s] view wasn’t realistic. It’s good to see also the danger of technology”.²³⁹

²³² Interview with Ethical Hacker A.

²³³ Interview with Ethical Hacker B.

²³⁴ Interview with Maker J.

²³⁵ Interview with Hactivist D.

²³⁶ Interview with Maker E.

²³⁷ Interview with Hactivist E.

²³⁸ Interview with Maker J.

²³⁹ Interview with Maker D.

The hackers I met also tend to have a commonsensical approach to the subject of voting and elections. Maker H argues that, “there are no good objective reasons why pencil and paper won’t suffice”.²⁴⁰ Maker J explains the problems with electronic voting: “You have to balance the costs to the improvement. I don’t see that there is such a big improvement in the process. It’s just a very high cost to implement this in a very secure way, and the risks they are just so great”.²⁴¹ From a practical standpoint, Maker J continues, “There’s no way. There’s no easy way to make a secure voting process in the same way we have right now.... The anonymity of it is too hard to implement”.²⁴² Hackers are aware of some of the advantages of electronic voting: “the modern character and administrative efficiency and advantages of these machines: easy, push-button voting, reduction of the number of polling stations, fast delivery of results”.²⁴³ However, they believe that the attendant risks of electronic voting far outweigh its benefits. Ethical Hacker A remarks, “If some kind of politician decides that democracy is, I don’t know, too expensive and we need voting computers. Or we vote once in four years but we cannot wait for an extra hour”.²⁴⁴ Hactivist D concurs, “you’re comparing four hours quicker results, and you don’t really think about the costs at all”.²⁴⁵

The security of elections is considered a serious matter for hackers since it concerns the validity and legitimacy of democratic rule and governance. According to the members of the campaign against voting computers: “Any vulnerabilities discussed herein affect the very foundations of our democracy.... In the case of a voting system, it is obvious that any lack of security has the potential to directly affect all of society”.²⁴⁶ Hactivist F agrees, “The integrity of the voting system,

²⁴⁰ Interview with Maker H.

²⁴¹ Interview with Maker J.

²⁴² Interview with Maker J.

²⁴³ Bart Jacobs and Wolter Pieters, “Electronic Voting in the Netherlands” 3.

²⁴⁴ Interview with Ethical Hacker A.

²⁴⁵ Interview with Hactivist D.

²⁴⁶ Rop Gonggrijp and Willem-Jan Hengeveld, “Studying the Nedap/Groenendaal ES3B voting computer” 2.

you need to be sure of in a democracy”.²⁴⁷ As a hacker acerbically puts it: it is never a good idea “to fuck around with voting and elections”.²⁴⁸ Hackers and politicians alike are keenly aware that “once trust in the voting system declines, it is hard to win this back. Without this support, the legitimacy of the chosen legislator will diminish” and so too the democratic foundations of government and society.²⁴⁹

5.2.2.3 Leaktober

Aside from the electronic voting computers campaign, Leaktober (in Dutch *lektober*) is another noteworthy case of hackers resisting or changing the law through hacking. Leaktober, a portmanteau of the words leak and October, illustrates how hacking can influence technology laws and policies. As the term suggests, the aim of this campaign was to make public a computer security leak or vulnerability of a government or company website or IT system every day in October 2011.²⁵⁰ Leaktober was principally carried out by Brenno de Winter, a well-known “hacker-journalist”, together with the IT news website Webwereld.²⁵¹ The impetus for Leaktober was their frustration with receiving daily reports about security vulnerabilities and leaks that could have been easily prevented or fixed.²⁵² The goal of the campaign then was to bring greater public attention to these vulnerabilities and to force government and companies to take action and improve the security of their systems.²⁵³ In order to disclose the security vulnerabilities responsibly, de Winter and Webwereld informed the affected party before they published any information.²⁵⁴ In addition, they did not copy or publicly release any personal data or information that they

²⁴⁷ Interview with Hacktivist F.

²⁴⁸ Interview.

²⁴⁹ Leontine Loeber, “E-Voting in the Netherlands” 29.

²⁵⁰ Nicole van der Meulen and Arno Lodder, “Cybersecurity”.

²⁵¹ Sander van der Meijs, “Leaktober: iedere dag een privacylek” <<http://webwereld.nl/beveiliging/54847-lektober-iedere-dag-een-privacylek-op-webwereld>> accessed 16 June 2015; see also Interview with Maker B (who uses the term “hacker-journalist” to describe Brenno de Winter); see also Nico van Eijk, “Datalekken: een reality check” 30.

²⁵² Sander van der Meijs, “Leaktober: iedere dag een privacylek” <<http://webwereld.nl/beveiliging/54847-lektober-iedere-dag-een-privacylek-op-webwereld>> accessed 16 June 2015.

²⁵³ Sander van der Meijs, “Leaktober: iedere dag een privacylek” <<http://webwereld.nl/beveiliging/54847-lektober-iedere-dag-een-privacylek-op-webwereld>> accessed 16 June 2015.

were able to gain access to through their security testing.²⁵⁵ The primary targets of Leaktober were government websites, particularly those of municipalities and cities.²⁵⁶ As Maker D explains, de Winter “called the city... each day, each week, saying your security is broken.... But he published it also online so the whole world could see the city... had a data leak that day”.²⁵⁷ The aim of disclosing a security leak per day was easily met since many government websites and online services were vulnerable to easily exploitable weaknesses.²⁵⁸ Leaktober quickly achieved its objective because, once informed of the breaches, the affected organizations including the Association of Dutch Municipalities immediately took down their websites and services and sought to fix them.²⁵⁹

Leaktober is of great import to the hackers that I met because, not only did it actually raise awareness about computer leaks and make the government and companies take action, but it promoted the norms and values of security and privacy. Some consider it an act of hacktivism because “people became more aware. It was more of a campaign, a strategic hacking for raising awareness, making those sites more secure”.²⁶⁰ Many hackers support the objectives and tactics of Leaktober and think very highly of de Winter and what he was able to accomplish. According to Maker D, “Brenno de Winter did good things for society, yeah. By proving that we have a lot of ICT problems and he brings them in the open”.²⁶¹ Maker B adds, “He found leaks, holes in the security, and then he told this to the cities. And he made a public fuss about it.... He was proving [to the] cities that their com-

²⁵⁴ Sander van der Meijs, “Lekttober: iedere dag een privacylek” <<http://webwereld.nl/beveiliging/54847-lekttober-iedere-dag-een-privacylek-op-webwereld>> accessed 16 June 2015.

²⁵⁵ Sander van der Meijs, “Lekttober: iedere dag een privacylek” <<http://webwereld.nl/beveiliging/54847-lekttober-iedere-dag-een-privacylek-op-webwereld>> accessed 16 June 2015.

²⁵⁶ Nicole van der Meulen and Arno Lodder, “Cybersecurity”.

²⁵⁷ Interview with Maker D.

²⁵⁸ Brenno de Winter, “Lekttober superknaller: Megalek treft 50 gemeenten” <<http://webwereld.nl/beveiliging/54950-lekttober-superknaller-megalek-treft-50-gemeenten>> accessed 16 June 2015; see also Nicole van der Meulen and Arno Lodder, “Cybersecurity”.

²⁵⁹ Brenno de Winter, “Lekttober superknaller: Megalek treft 50 gemeenten” <<http://webwereld.nl/beveiliging/54950-lekttober-superknaller-megalek-treft-50-gemeenten>> accessed 16 June 2015; see also Nicole van der Meulen and Arno Lodder, “Cybersecurity”.

²⁶⁰ Interview with Maker B.

²⁶¹ Interview with Maker D.

puter systems, websites were not secure”.²⁶² The hacking activities that were carried out as part of Leaktobber ultimately helped improved the security of many IT systems. “Yeah, it was successful because they still talk about it, and they are more aware of it”, continues Maker B.²⁶³

The affected organizations, including municipal governments, were not too pleased with being the subject of public naming and shaming. As Maker B relates, “In the media, in the public, they were of course not so happy but they were admitting that it was important and they would work on it... But behind the doors of course they were not so polite, I think”.²⁶⁴ But, in the end, the municipal governments accepted the fact that they needed to prioritize security and makes changes. According to Maker D, “the city... said well you’re welcome, because it’s only testing our ICT and it’s very good”.²⁶⁵ Despite its success in changing government policy and forcing government action to improve computer security, Leaktobber also produced unexpected results for hackers. One of the unintended effects of Leaktobber was that, by raising awareness of security issues, some hackers believe that it also made the general public more afraid and fearful of hackers and hacking. As Maker G explains, “Yeah it might have made people aware and also... afraid, is my web shop going to be the next one”.²⁶⁶ Furthermore, in the wake of Leaktobber, both the public and the main-stream press were no longer interested in the issue security leaks “because of lektobber, it wasn’t newsworthy” anymore.²⁶⁷ It appears that, after Leaktobber, it is harder for hackers to receive the same level of media coverage and public attention for publicizing security vulnerabilities and to get the government or the public to take action.

²⁶² Interview with Maker B.

²⁶³ Interview with Maker B.

²⁶⁴ Interview with Maker B.

²⁶⁵ Interview with Maker D.

²⁶⁶ Interview with Maker G.

²⁶⁷ Interview with Maker G.

5.2.2.4 Hacking the OV-chipcard

Among the hackers I spoke to, the positive outcomes of the voting computers campaign and Leaktober are often contrasted with their inability to prevent the introduction and use of the Dutch national public transport card (the OV-chipcard or OV-chipkaart in Dutch)²⁶⁸ despite the numerous objections and hacks against it. The OV-chipcard is “a common means of payment for all forms of public transport in The Netherlands” and has a “contactless chipcard, which can be loaded with a balance in Euros and specific travel products”.²⁶⁹ The roll out and use of this “smart card based e-ticketing system for all forms of public transport: bus, train, metro, etc.” within the Netherlands has been and continues to be a hotly debated and highly contested topic ever since security issues with the card gained widespread public and media attention in 2007.²⁷⁰ “The stakes are high” with respect to the OV-chipcard, writes Jacobs, “the invested economical and political interests and the prestige at risk are high”.²⁷¹ In addition, the OV-chipcard involves many public and private stakeholders and interests:

because there are so many public transport companies, public authorities (at various levels, local, regional, national) and stakeholders involved. Various motivations for such a card exist: fair division of revenues and/or subsidies and improvement of service via detailed travel logs, public safety via restricted access (via electronic gates), fraud reduction, cost reduction (fewer inspectors needed), convenience for travelers, behavioural targeting and direct marketing via personal travel profiles, and simply the desire to look modern and high-tech.²⁷²

Ethical Hacker B explains, “that was really a hot item because it cost like a billion Euros. It was funded by public money. Nobody really

²⁶⁸ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 291; see also “OV-chip” <https://ovchip.cs.ru.nl/Main_Page> accessed 18 February 2015.

²⁶⁹ TNO, “Security Analysis of the Dutch OV-ChipKaart” 3.

²⁷⁰ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 291-292; see also “OV-chip” <https://ovchip.cs.ru.nl/Main_Page> accessed 18 February 2015; see also Leontine Loeber, “E-Voting in the Netherlands” 29.

²⁷¹ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 294.

²⁷² Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 292.

wanted it, but it was still pushed”.²⁷³ Hactivist A adds, “None of the citizens actually asked for this system. Many of them protested against the privacy violations. The government ignored it”.²⁷⁴

Between May 2007 and March 2008, the security of the various underlying technologies of the OV-chipcard was compromised on four separate occasions by three different groups of security researchers and students connected with universities in the Netherlands, Germany and the United States.²⁷⁵ Basically, the researchers found that the security of the card, which relied on “a proprietary authentication protocol and stream cipher using [encryption] keys”, could be broken or circumvented with the right tools or techniques.²⁷⁶ This meant that once the security of a card was compromised, an attacker could, among other things, gain access to and steal a cardholder’s personal data and travel information that are stored on the card, fraudulently top-up the value on the card, or create cloned or fake cards.²⁷⁷ In all four cases, the findings and security reports of the students and security researchers were disclosed to the general public as well as the entities responsible for rolling out the OV-chipcard.²⁷⁸ Hactivist A recalls,

A bunch of experts in this area – these students and professors – wrote a letter to the Ministry saying, ‘Look, this is not a good plan. This is going to be hacked 6 ways to Sunday on day 1 of implementation. So either pick a new technology or start over’. And that letter was ignored. Then they sent follow-up letters. And the follow-up letters, they were also all ignored.²⁷⁹

However, the company that produced the chips for the cards, NXP Semiconductors, sought a court injunction to stop the security re-

²⁷³ Interview with Ethical Hacker B.

²⁷⁴ Interview with Hactivist A.

²⁷⁵ “OV-chip” <https://ovchip.cs.ru.nl/Main_Page> accessed 18 February 2015; see also TNO, “Security Analysis of the Dutch OV-ChipKaart” 3.

²⁷⁶ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 292; see also Adrian Cho, “University Hackers Test the Right To Expose Security Concerns” 1322-1323.

²⁷⁷ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 292-294; see also TNO, “Security Analysis of the Dutch OV-Chipkaart” 5, 6, 11 and 12.

²⁷⁸ “OV-chip” <https://ovchip.cs.ru.nl/Main_Page> accessed 18 February 2015; see also Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 292.

²⁷⁹ Interview with Hactivist A.

searchers at Radboud University Nijmegen from releasing their results.²⁸⁰ The Dutch court ruled against NXP Semiconductors and held that the research could be published on the grounds that the “the chance of damage must be attributed largely to the production and entry into service of a chip with intrinsic defects, which is the responsibility of NXP and not of Radboud University Nijmegen who only laid bare [such defects] by research” and the finding and disclosure of security vulnerabilities “is to some extent something that in an open democratic society should be accepted”.²⁸¹

A few years later, the OV-chipcard was once again in the news when journalist Brenno de Winter wrote about how he was able to travel for three weeks using a cracked OV-chipcard.²⁸² A hacker explains how cracked cards are used:

You can take a cash, pre-paid bought OV-chipkaart and you can just charge it up with whatever you want. Or you can check yourself in, at a station, and then you get on a train, and you go to the other side of the country and when the conductor comes, your card says that you are checked in.²⁸³

Doing it for journalistic purposes and to show the relative ease of breaking the OV-chipcard,²⁸⁴ de Winter even got Members of Parliament to travel using cracked or fake cards. Maker H recounts how de Winter “had several Members of Parliament travel for a few weeks with fake OV-chipkaarts, so using their parliamentary immunity”.²⁸⁵

Despite the many attempts by hackers and security researchers to stop the implementation and use of the OV-chipcard through hack-

²⁸⁰ Adrian Cho, “University Hackers Test the Right To Expose Security Concerns” 1322; see also Elinor Mills, “Dutch chipmaker sues to silence security researchers”.

²⁸¹ NXP Semiconductors vs Radboud Universiteit Nijmegen, Arnhem Court Case Number 171900 (18 July 2008) 4.20 and 4.23; see also Elinor Mills, “Dutch court allows publication of Mifare security hole research”; see also Adrian Cho, “University Hackers Test the Right To Expose Security Concerns” 1322.

²⁸² Sander van der Meijs, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <<http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart>> accessed 16 June 2015.

²⁸³ Interview.

²⁸⁴ Sander van der Meijs, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <<http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart>> accessed 16 June 2015.

²⁸⁵ Interview with Maker H.

ing and exposing its security vulnerabilities, on the whole, these hacks have not produced the desired effect. The hacks have had “little direct impact on the actual roll-out of the OV-chipkaart” aside from “some additional delays, and in the development of a migration plan”.²⁸⁶ According to Jacobs, “After a phase of denying, dismissing and trivialising these findings the main players started accepting them and began working on a replacement plan towards a new card. In the meantime the actual roll-out went ahead”.²⁸⁷ So, while disclosing security issues resulted in “a lot of pressure from Parliament” and “delayed the introduction of” the OV-chipcard,²⁸⁸ hackers admit that “the situation itself didn’t change”.²⁸⁹ At most, the hacks raised awareness about the card’s security issues and forced technical improvements specifically in relation to fraud prevention.²⁹⁰ As Jacob writes, “In the Netherlands politicians and industrials have become aware of the fact that large ICT-projects can be made or broken by security issues”.²⁹¹ Maker H notes that the companies who were responsible for the OV-chipcard “were receptive, responsive to that, and replaced the old vulnerable card to much more modern cards which... undoubtedly also have their weaknesses”.²⁹² Maker L adds, “they took some action with it to make it better. But yeah, I hoped it would have more effect. I hoped”.²⁹³ As Maker J points out though, “the end result was that [it] improved the security a little bit, but the fundamental problems... are not solved”.²⁹⁴

For the hackers I spoke to, the fundamental problems of the OV-chipcard concern both security and privacy. They do not trust the OV-chipcard to protect their privacy because it is not secure. “The system is fundamentally broken. It is ridiculously easy to hack.

²⁸⁶ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 295.

²⁸⁷ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 292.

²⁸⁸ Interview with Maker L.

²⁸⁹ Interview with Maker J.

²⁹⁰ TNO, “Security Analysis of the Dutch OV-ChipKaart” 11-12; interview with Hacktivist E; interview with Ethical Hacker B.

²⁹¹ Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 295.

²⁹² Interview with Maker H; see also TNO, “Security Analysis of the Dutch OV-ChipKaart” 12.

²⁹³ Interview with Maker L.

²⁹⁴ Interview with Maker J.

It doesn't take a lot of effort", points out Hacktivist A.²⁹⁵ Moreover, they believe that the card infringes on their privacy because copious amounts of data are collected about them and they can be profiled and their movements monitored. Despite the disclosures of security vulnerabilities, members of the hacker community admittedly were not able to control the debate and change public opinion. Rather than focusing on privacy issues, public discussions centered mainly on how the security issues could lead to fraud through the creation and use of fake or cracked cards. As Ethical Hacker B notes, the companies who were behind the OV-chipcard, "one of the main things they used as propaganda was like we move to this because then we don't have any people traveling without paying".²⁹⁷ But as Maker H points out, "The fundamental issue with the OV-chipkaart is not fraud".²⁹⁸ Maker G agrees, "my objection with the OV-chipkaart is not that you can fake, you can cheat. But it's more that, it's just electronic registration of your movements".²⁹⁹ Maker H claims that

The fundamental issues with the OV-chipkaart are not necessarily, were not really affected by the vulnerabilities in the card itself. It didn't really affect the fundamental question, at least one of the fundamental questions of the OV-chipkaart. I would say almost unprecedented collection about... physical movement of people.³⁰⁰

The privacy concerns about the OV-chipcard stem from the fact that, as explained by Jacobs, "the OV-chip smart card based e-ticketing system involves a centralised architecture giving the travel companies unprecedented access to individual travel behaviour".³⁰¹ Jacobs explains the specifics of how the OV-chipcard system works:

each entry or exit into the public transport system, in a bus or at

²⁹⁵ Interview with Hacktivist A.

²⁹⁶ See TNO, "Security Analysis of the Dutch OV-ChipKaart" 11-12.

²⁹⁷ Interview with Ethical Hacker B.

²⁹⁸ Interview with Maker H.

²⁹⁹ Interview with Maker G.

³⁰⁰ Interview with Maker H.

³⁰¹ Bart Jacobs, "Security and Privacy Issues in Transport and Beyond" 294.

a train station, generates an entry in the back-office of the travel companies, involving among others the identity of the entry/exit point (often connected to a fixed location), time-of-day, and identity and balance of the card. This yields a huge database of travel transactions that can often be linked to specific clients, for personalised cards. Hence individual travel patterns can be determined easily. The travel companies have left no doubt that they are quite eager to do so and to use these data for behavioural targeting and direct marketing.³⁰²

Hactivist B points out, “Then you get to the more fundamental problem of the OV-chipkaart”.³⁰³ Hactivist B continues:

One of the major failures with the whole thing about the OV-chipkaart was that in publicizing how the chip was hackable, really the only thing they disclosed was a very private problem for the company exploiting this card that they were susceptible to a means of fraud.... They didn’t expose any form of critique on the data gathering or anything. It was just we can travel for free. Why is this a problem?³⁰⁴

Hactivist A concurs, “The privacy implications of that are just horrendous. Think, a central database run by a private company that is not on a democratic oversight, that now stores, and God knows what they do with the data. They might be reselling it. They might not be securing it properly”.³⁰⁵ According to Maker G, “unless people really see a threat in this, I don’t know if this can change”.³⁰⁶

Some hackers believe that there’s no point in hacking the OV-chipcard any further: “Yeah, hacking it again doesn’t prove a point anymore... already proven the point”.³⁰⁷ However, others believe that there could have been better tactics that would have placed the issue of privacy squarely on center stage. For example, a hacker imagines how “it would have been way more interesting if someone were to hack

³⁰² Bart Jacobs, “Security and Privacy Issues in Transport and Beyond” 293.

³⁰³ Interview with Hactivist B.

³⁰⁴ Interview with Hactivist B.

³⁰⁵ Interview with Hactivist A.

³⁰⁶ Interview with Maker G.

the database and just dump that online and like, here you go fuckers".³⁰⁸ While mindful of the ethical, social and legal consequences, the hacker contends, "Then you immediately get the question of if it's not OK to integrally dump this online, why is it OK if the NS [national railway company] keeps track of this and sells this data to other private companies?".³⁰⁹

5.2.3 WORK WITH, USE AND ADAPT

While it is may not be their preferred approach, the hackers I met are also open to pursuing legal means, which may include working with, using or adapting the law tactically to achieve their goals. The two examples discussed below do not technically involve hacking since they are primarily concerned with changing and using laws and policies rather than technology per se. These cases also required working within the legal system and according to established legal procedures and rules. Nevertheless, the actions and activities that hackers carried out in relation to these cases were still very much grounded on and impelled by hacker culture and in furtherance of their norms and values. In addition, the targets of these cases were not simply general laws but specific technology laws and policies that are germane to hacking.

5.2.3.1 Net neutrality rules

The hacker community played a key role in the enactment of net neutrality legislation in the Netherlands as they lobbied and worked with Members of Parliament to get the law passed. The campaign to introduce a formal net neutrality law was mainly led by Bits of Freedom, a digital rights organization that has relatively strong ties with hackers. In fact, some hackers consider Bits of Freedom to be a part of the hacker community since the organization was re-launched during

³⁰⁷ Interview with Maker L.

³⁰⁸ Interview.

³⁰⁹ Interview.

the quadrennial Dutch outdoor hacker conference in 2009³¹⁰ and it was very active during the same hacker conference in 2013, particularly at the more political NoisySquare village.³¹¹ Moreover, the organization counts a number of hackers as its volunteers or members. Maker L claims that, “Bits of Freedom comes from the hacker community”.³¹²

Bits of Freedom began its net neutrality campaign in 2009 when it published a position paper encouraging the adoption of net neutrality principles and rules.³¹³ However, it was only in April 2011 when a controversy broke out about the use of deep packet inspection (DPI) by the dominant Dutch telecommunications provider KPN to monitor the internet activities of its customers and the applications and services that they used that the campaign finally gained traction and widespread attention of legislators and the public.³¹⁴ The spark came when an executive at KPN mentioned during a meeting with the company’s investors that it had DPI technology that could be used to monitor the internet traffic of its customers and potentially charge them tariffs for using messaging services like WhatsApp in order to offset the company’s declining voice and SMS revenues.³¹⁵ A lawyer from Bits of Freedom, Janneke Sløetjes, explains, “KPN was proud to announce that they used DPI to determine which kind of websites

³¹⁰ Joris van Hoboken, “Relaunch Bits of Freedom!” <<http://www.jorisvanhoboken.nl/?p=300>> accessed 24 August 2015; see also Bits of Freedom “Nieuwsbrief Nr. 6.15” <<https://www.bof.nl/live/wp-content/uploads/nieuwsbrief160810.txt>> accessed 24 August 2015.

³¹¹ OHM2013, “Village:Noisy Square” <https://ohm2013.org/wiki/Village:Noisy_Square> accessed 24 June 2015.

³¹² Interview with Maker L.

³¹³ Bits of Freedom, “Position Paper Netwerkneutraliteit” <<https://www.bof.nl/live/wp-content/uploads/Position-Paper-netneutraliteit.pdf>> accessed 24 June 2015; see also Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 9.

³¹⁴ Andreas Udo de Haes, “KPN luistert abonnees af met Deep Packet Inspection” <<http://webwereld.nl/beveiliging/53691-kpn-luistert-abonnees-af-met-deep-packet-inspection>> accessed 18 June 2015; see also Bits of Freedom, “Onze Successen” <<https://www.bof.nl/over-ons/onze-successen/>> accessed 18 June 2015; see also Parker Higgins, “The Netherlands Passes Net Neutrality Legislation” <<https://www.eff.org/declinks/2012/05/netherlands-passes-net-neutrality-legislation>> accessed 18 June 2015; see also Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 9; see also Kevin O’Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

³¹⁵ Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 5 and 9; see also Nico van Eijk, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015, 8; see also Archibald Preuschat, “KPN Admits To Using Deep Packet Inspection” <<http://blogs.wsj.com/tech-europe/2011/05/12/kpn-admits-to-using-deep-packet-inspection>> accessed 24 June 2015; see also Kevin O’Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

customers visited and then to offer specialized packages. It wasn't the case that they were necessarily doing it, but it was enough evidence for us".³¹⁶ Maker L narrates, "It was a great fight when they found the part of the interview with some shareholders of the KPN dude who said they want to do DPI to get people to pay for WhatsApp".³¹⁷ The significance of the controversy over DPI was that "people saw the negative outcomes that would be possible if you don't have net neutrality law. People were warning about that for a long time".³¹⁸

Bits of Freedom, together with hackers and the wider internet community,³¹⁹ seized the opportunity to fan the public outcry over KPN's use of DPI to demand the inclusion of net neutrality rules in the Telecommunications Act, which was coincidentally being revised by Parliament at the time.³²⁰ Maker L explains, "a lot of people in the hacker community worked together with Bits of Freedom, and Bits of Freedom was very vocal about that".³²¹ According to Bits of Freedom, "The use of DPI gained much attention when KPN admitted that it analysed the traffic of its users to gather information on the use of certain apps".³²² Sløetjes further recounts:

We were pushing net neutrality since 2009, but no one was listening. But that changed when KPN showed that they were using DPI, deep packet inspection. That's when BoF [Bits of Freedom] jumped on it. DPI is a violation of communications confidentiality. We told people to report crimes to the police, and they did. We had a draft law ready. It was short. The government was reviewing telecommunications law at the time, and there was room to add extra provisions. We're going just one step further. The government was not enthusiastic at first, but then they saw

³¹⁶ Roslyn Layton, "Net neutrality in the Netherlands: Dutch solution or Dutch disease?" 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 33; see also Archibald Preuschat, "KPN Admits To Using Deep Packet Inspection" <<http://blogs.wsj.com/tech-europe/2011/05/12/kpn-admits-to-using-deep-packet-inspection>> accessed 24 June 2015.

³¹⁷ Interview with Maker L.

³¹⁸ Interview with Hacktivist F.

³¹⁹ Interview with Maker J.

³²⁰ Bits of Freedom, "Onze Successen" <<https://www.bof.nl/over-ons/onze-successen/>> accessed 18 June 2015; see also Roslyn Layton, "Net neutrality in the Netherlands: Dutch solution or Dutch disease?" 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 10 and 11.

³²¹ Interview with Maker L.

³²² Ot van Daalen, "Netherlands First Country in Europe with Net Neutrality" <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

the advantages of it. It all happened because of the hype. It was a combination of being ready, KPN's announcement, and the telecom legislation on the table. We managed to blast the opportunity. We demonstrated the problem, showed what we wanted, and how to make it happen.³²³

According to a person knowledgeable about the campaign,

We had a very lucky break because the spokesperson from KPN... in a different context boasted about their ability to do deep packet inspection. Which then led to sort of a big media downfall and then allowed the law to pass very quickly.³²⁴

In a little over a year, the net neutrality campaigners were able to use the media attention and the public outrage (especially online) generated by the DPI controversy to effectively lobby the major political parties to adopt net neutrality provisions as part of the revision of European telecommunications law.³²⁵ The net neutrality law had the support of the majority of the Dutch Parliament,³²⁶ and was adopted by Parliament in May 2012 and took effect on 1 January 2013.³²⁷ The Netherlands thus became one of the first countries to have “specific net neutrality standards in place. It was the first country to do so in the European Union”.³²⁸ According to Ot van Daalen, the Director of Bits of Freedom at the time, “The net neutrality law prohibits

³²³ Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 5 and 34.

³²⁴ Interview.

³²⁵ Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 9 and 10; see also Nico van Eijk, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015, 10; see also Parker Higgins, “The Netherlands Passes Net Neutrality Legislation” <<https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation>> accessed 18 June 2015; see also Kevin O'Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

³²⁶ Kevin O'Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

³²⁷ Nico van Eijk, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015, 11; see also Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015; see also Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 11.

³²⁸ Nico van Eijk, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015, 7; see also Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015; see also Kevin O'Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015; see also interview with Maker L.

internet providers from interfering with the traffic of their users”.³²⁹ He further explains, “the law includes an anti-wiretapping provision, restricting internet providers from using invasive wiretapping technologies, such as deep packet inspection”.³³⁰

Bits of Freedom, other non-governmental organizations and members of the hacker community were all instrumental in the adoption of the net neutrality law.³³¹ A person who had intimate knowledge about the campaign relates how Bits of Freedom “wrote the key net neutrality provision”.³³² The person continues, “People were working on that. We were actively trying to find a political majority to pass an amendment on the Telecoms Act that we’ve basically written”.³³³ Higgins notes how the Dutch net neutrality rules came “after vigorous campaigning by civil society groups including influential digital rights group, Bits of Freedom”.³³⁴ Van Eijk confirms, “A lot of reactions were the result, advocating a more material, more concrete approach to net neutrality. These reactions were partly caused by a call from Bits of Freedom, a very active NGO, to react”.³³⁵ Maker L explains how “a lot of people talked to the parliament people and protested right way on Twitter and other things, and used their way to get it done”.³³⁶

Hackers supported and were actively involved in the campaign because they saw the net neutrality rules as playing a critical part in preserving freedom on the internet, which they consider essential for fostering greater techno-social creativity and innovation. One of the

³²⁹ Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

³³⁰ Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

³³¹ Roslyn Layton, “Net neutrality in the Netherlands: Dutch solution or Dutch disease?” 24th European Regional Conference of the International Telecommunication Society, Florence, Italy, 20-23 October 2013, 4; see also Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

³³² Interview.

³³³ Interview.

³³⁴ Parker Higgins, “The Netherlands Passes Net Neutrality Legislation” <<https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation>> accessed 18 June 2015.

³³⁵ Nico van Eijk, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015, 9-10; see also Parker Higgins, “The Netherlands Passes Net Neutrality Legislation” <<https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation>> accessed 18 June 2015.

³³⁶ Interview with Maker L.

main goals of net neutrality is “to safeguard an open and secure internet in The Netherlands” because “Internet access is very important for functioning in an information society”.³³⁷ According to the explanatory memorandum on the net neutrality provisions:

This restriction on the behavior of providers of Internet services is necessary to ensure open and unrestricted access to the Internet for (online) service providers, citizens and business. It should be prevented that Internet access service providers block or restrict specific information or services.³³⁸

Echoing the sentiment of many hackers, the Dutch deputy prime minister, Maxime Verhagen, told the press that: “The blocking of services or the imposition of a levy is a brake on innovation.... That’s not good for the economy. This measure guarantees a completely free Internet which both citizens and the providers of the online services can then rely on”.³³⁹ Furthermore, the net neutrality rules concern the all-important hacker norms and values of freedom of access, individual autonomy and liberty, and privacy (to use the internet without being monitored). These norms and values are recognized in the explanatory memorandum as well. For instance, it states that, “End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes”.³⁴⁰ The explanatory memorandum further highlights the need to preserve or “to maximise choice and freedom of expression on the Internet for end users”.³⁴¹ According to Bruno Braakhuis, the Member of Parliament who originally sponsored the net neutrality rules, “For us, this is really a basic right... We consider network neutrality to be as important as freedom of the press, freedom

³³⁷ Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

³³⁸ Bits of Freedom, “Translations of Key Dutch Internet Freedom Provisions” <<https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/>> accessed 18 June 2015.

³³⁹ Kevin O’Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

³⁴⁰ Bits of Freedom, “Translations of Key Dutch Internet Freedom Provisions” <<https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/>> accessed 18 June 2015.

³⁴¹ Bits of Freedom, “Translations of Key Dutch Internet Freedom Provisions” <<https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/>> accessed 18 June 2015.

of speech”.³⁴²

A number of hackers were part of net neutrality campaign and they are quite proud of their achievement.³⁴³ As Maker L proclaims, “I think one thing that was a big success in the Netherlands is the net neutrality law.... I think we hacked us a nice law, [got] the politics right to get that law enacted”.³⁴⁴ Some hackers consider it “probably our biggest success, most impactful success” in terms of changing technology law and policy.³⁴⁵ They proudly claim that the Dutch net neutrality law has become “the model inside the EU for the people who support true net neutrality as something to try to get enacted over there as well”.³⁴⁶ Many hackers admittedly share Maker J’s sentiment that, “I think it was sort of a surprise in how well it was actually implemented”.³⁴⁷ They concede though that the net neutrality campaign “was a very legal approach to the problem rather than” hacking and “the majority of it was advocacy and policy work done by legal people” and not hackers.³⁴⁸ While some hackers consider this a deficiency, on the contrary, I believe this perfectly illustrates how hackers, lawyers and government officials can work together to develop and improve technology laws and policies. My position is further elucidated in the discussions on responsible disclosure and open data in Sections 6.2.1 and 6.2.2.

³⁴² Kevin O’Brien, “Dutch Lawmakers Adopt Net Neutrality Law” <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015.

³⁴³ Interview with Maker J; interview with Maker L.

³⁴⁴ Interview with Maker L.

³⁴⁵ Interview with Hacktivist F.

³⁴⁶ Interview with Hacktivist F; see also Ot van Daalen, “Netherlands First Country in Europe with Net Neutrality” <<https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/>> accessed 18 June 2015.

³⁴⁷ Interview with Maker J.

³⁴⁸ Interview with Hacktivist F.

5.2.3.2 Open source projects

As explained in Section 2.2.4 on FOSS developers, hackers use copyleft and FOSS licenses not merely to subvert intellectual property laws but also to constructively change and adapt these legal rules to serve and support various hacker norms and values. For instance, the development of open source projects and the use of FOSS licenses help promote openness and freedom of access, which enable fellow hackers and members of the public to freely use, build on and share their creations and innovations. According to Maker I, “If a project I’m working with it’s not a closed source project, that’s an open source project or a free software project, people who want to participate are able to participate. So it’s not a closed group”.³⁴⁹ Open source projects can also advance the norms and values of efficiency and creativity and innovation. Hactivist B underscores the ability of open source to create “products comparable and even better quality-wise to those produced within the capitalist framework, but completely volunteer-based”.³⁵⁰ Hactivist D likewise says, “We have people who would say I like open source because it allows me to build up my own project... I just think it’s cool to have all of this free code which I can use and hack”.³⁵¹ Maker I explains the essential role open source plays in supporting community development and social development: “Yes, I think open source is really important. I look at it at two ways. I think, in itself, open source is a process which is a good thing. For society, it’s important [and] has a good effect”.³⁵² Maker I continues, “the benefits definitely include also access to a lot of knowledge and enthusiasm and also I would say social capital”.³⁵³ Open source is undeniably a core practice and ethos among hackers. Hactivist B recounts how the use of open source “was really one of the core values” when they established their hackerspace.³⁵⁴ Maker I adds, “There’s a lot of open source

³⁴⁹ Interview with Maker I.

³⁵⁰ Interview with Hactivist B.

³⁵¹ Interview with Hactivist D.

³⁵² Interview with Maker I.

³⁵³ Interview with Maker I.

³⁵⁴ Interview with Hactivist B.

values and culture in, for example, all of the entrepreneurs who come from the RepRap community”.³⁵⁵

The use of free and open source technologies and licenses remains strong among makers and hacktivists that I met, and many Dutch hackers consciously or by default choose to use and work on open source projects, particularly in relation to open source hardware. There is a very active RepRap community in the Netherlands that continues to build and develop this open source 3D printer.³⁵⁶ The Ultimaker 3D printer, which is based on RepRap and is developed by Dutch makers, is often cited as the poster child of open source hardware since, unlike MakerBot, the hardware and software of Ultimaker remain completely open source and everybody is free to work and build on it.³⁵⁷ Maker G explains that, when working on projects, “I try to just make it open source.... Well it’s nice so I use open source software myself”.³⁵⁸ According to Maker K, “I know most people who develop stuff just goes under the Creative Commons license”.³⁵⁹ Similarly, Ethical Hacker B relates how “I made all those open source. I just pushed it into the community. Like ok, everybody can start playing with it”.³⁶⁰

Open source technologies and practices have admittedly become prevalent and influential both within and outside the hacker community. Maker D narrates how “we don’t try to lobby as hard for open source as before because the industry of open source is now very good and very self-containing. So it’s not the highest priority”.³⁶¹ Maker D continues, “Open source was really important, but open source has matured, the market has matured”.³⁶² Some hackers though remain

³⁵⁵ Interview with Maker I.

³⁵⁶ Interview with Hactivist C.

³⁵⁷ Anna Kazianus France, “Shiny! New! Ultimaker 2!” <<http://makezine.com/2013/12/06/in-the-shed-shiny-new-ultimaker-2/>> accessed 22 July 2015; see also 3D Hubs Blog, “Open Source 3D Printers stand up to giants Stratasys and 3D Systems” <blog.3dhubs.com/post/66187555251/open-source-3d-printers-stand-up-to-giants-stratasys> accessed 27 November 2013.

³⁵⁸ Interview with Maker G.

³⁵⁹ Interview with Maker K.

³⁶⁰ Interview with Ethical Hacker B.

³⁶¹ Interview with Maker D.

³⁶² Interview with Maker D.

frustrated by the absence of a formal government policy on open source. Since the early 2000s, hackers have been lobbying the Dutch government to enact policies on the adoption and use of open source software.³⁶³ “They were talking about implementing it. It was all, it was all mostly still talking. Which was good, which is always where everything begins”, recounts Hactivist A.³⁶⁴ While the discussions were initially promising, “certainly, by the summer of 2010, it was dead in the water.... That’s been completely killed” possibly due to pressure from powerful political and economic interests.³⁶⁵ Nevertheless, open source has proven to be very resilient in relation to particular legal issues. “Intellectual property law does affect that [open hardware movement] and likewise with software development in general”, Maker H explains, “But thanks to all of the work done in the open source, free software movement, that is much less of an issue nowadays than it used to be”.³⁶⁶ In fact, open source has also been used as tactic or defense against legal actions and restrictions. A hacker explains how “a lot of guys are just like doing whatever the hell they want and then kind of use like open source as an inoculation against” potential legal liability.³⁶⁷ “No big company wants to sue an open source company”, continues the hacker, “it’s a defense, a PR defense and people actively use it”.³⁶⁸ Using open source as a kind of incantation to dispel legal issues, “you can inoculate yourself against it by saying, ‘Hey we’re open source man’... You cannot go on the record in today’s tech community and do anything anti-open source”.³⁶⁹

Despite its influence and creative uses, open source is far from being immune to all legal problems and conflicts. For example, patents remain a critical issue for open source projects. Within the “open

³⁶³ Interview with Hactivist A.

³⁶⁴ Interview with Hactivist A.

³⁶⁵ Interview with Hactivist A.

³⁶⁶ Interview with Maker H.

³⁶⁷ Interview.

³⁶⁸ Interview.

³⁶⁹ Interview.

source community, it seems like we also have to get patents to be able to sustain ourselves”, explains Maker I, “We feel that’s a problem if we get patents because we are at least on some level against that” because patents can restrict openness and freedom of access.³⁷⁰ Nonetheless, Maker I notes how openness can also be employed to defeat the restrictions of patents: “I don’t think there’s a lot of protection [for open source]. There’s at least one protection that I know of, by publishing you create prior art”.³⁷¹ So, by publicly releasing and sharing their inventions and technological creations online, makers can prevent others from patenting and closing off an invention and exercising exclusive rights over it. “That’s one thing, one reason to be open sourcing something and making a project out of it”, explains Maker I.³⁷²

5.3 Complex relations and reactions

As evinced by the above perceptions, attitudes and responses of hackers to law, the relationship between hacking and the law can be characterized as multifaceted, complicated and ostensibly paradoxical. Do hackers consider laws to be irrelevant? Would hackers prefer a world without laws? Do hackers loathe public authorities? Are laws and public authorities antithetical to hacking? As this chapter has shown, such questions cannot be satisfied with simple yes or no answers since they demand more nuance and contextualization. As seen in the campaign against electronic voting machines, hackers can strive to change technology laws and policies that they disagree with through technical means. But, they can also utilize or work within the legal system to change and improve laws, as demonstrated by the adoption of the net neutrality legislation in the Netherlands and the continued development and use of open source projects and licenses to counteract the restrictions and restrictive uses of intellectual property laws

³⁷⁰ Interview with Maker I.

³⁷¹ Interview with Maker I.

³⁷² Interview with Maker I.

and rights. So, while the relations between hacking and the law may be far from cordial, they are not completely adversarial. In certain cases, hackers are willing to work with the public authorities if they believe that such projects or activities will have a social impact and redound to the benefit of their community and the wider public. Hackers generally prefer to focus on developing their technologies and communities, but, as a practical matter and as a means to an end, they are ready to engage with law and public authorities to resolve critical issues that affect hacker norms and values and impact society as a whole.

Makers and hacktivists value their individual autonomy and liberty, yet they are also socially conscious and they recognize the importance of using their rights to protect the freedoms of others and to advance community and social development. Furthermore, even though the hackers I met may have problems with law and authority due to their non-conformist and anti-establishment attitudes, they are surprisingly open to knowing more about the law, receiving greater legal protection for their fundamental rights and freedoms, and even ensuring the integrity of a system that elects public officials. This apparent incongruity can be explained by the fact that hackers perceive and approach the law and authority in two distinct ways: restrictive or unjust laws and governments must be opposed, while laws and systems that uphold basic human rights and promote democratic freedoms and processes should be supported. It is true that many hackers that I met are not fond of politics or politicians, but they view hacking as a political act and they, for the most part, subscribe to the ideals and values of democracy.

Gaining a more nuanced, dense and empirically grounded understanding of the complex and competing relationship and interactions between hacking and law is paramount and a necessary prerequisite in order to reasonably determine and properly prescribe optimal approaches to the regulation and governance of hacking. The succeed-

ing chapter discusses the normative implications and legal recommendations of the research.

CHAPTER SIX

Normative conclusions and legal recommendations

This chapter sums up the normative implications of the research and puts forward legal recommendations on how to improve technology laws and policies concerning hacking. It proposes changes in the way makers and hacktivists and law and public authorities view and respond to each other. Despite their complex and conflicting relations, they can resolve their differences by building on their shared values, having a more open and empathetic view of and reaction to the other, and working as partners in the development of technology laws and policies.

6.1 Normative implications

6.1.1 HACKERS AS TECHNICAL, SOCIAL AND LEGAL ACTORS

As borne out by the empirical findings and analysis in the preceding chapters, makers and hacktivists are highly technical yet socially aware individuals and communities. Technology lies at the heart of their culture and all of their practices and activities involve or revolve around it. Hackers are exceedingly passionate about technology and they desire to understand how it works in order to improve their personal knowledge and skills and also to produce something new, innovative or surprising from it. The hackers I observed were hacking and

building all sorts of technologies from 3D printers and other digital fabrication tools to encryption and security software. While the hackers I met can admittedly be playful and cause some disruption with their hacking projects and activities, they are not motivated by malice and they do not willfully or intentionally cause damage. They are simply curious about technology and what interesting things they can do with it. Despite their seemingly inordinate focus and possibly even obsession with technical matters, makers and hacktivists are very socially conscious and responsible. They are quite sociable, have a strong sense of community, and care much about the impact of technology on society. Even though they cherish the personal values of creativity and innovation, curiosity and individual autonomy and liberty, in practice, these always go hand-in-hand with the more communitarian goals of community development and social development. For example, makers may get personal gratification from building a laser cutter or CNC machine from scratch but they are not completely satisfied with their work unless they are able to share what they learned with others and their creations have a positive impact on society. Similarly, hacktivists do their utmost to protect not only their own security and privacy but also those of others.

The makers and hacktivists I met are not only internally and community focused, but also outwardly and socially oriented. While they may have issues with public authorities and certain hacking-related laws, they are willing to engage with and change technology laws and policies so as to uphold and protect fundamental rights and freedoms and democratic values. As seen in Chapter 5, hacktivists hacked the electronic voting machines to protect the right to vote and the secrecy of the ballot and preserve the validity of the electoral system. In the cases of Leaktobber and the hacking of the OV-chipcard, hackers sought to highlight and safeguard the important values of security and privacy in public and private information systems. Furthermore,

through the net neutrality campaign and the development and use of open source projects, hackers worked within the legal system to achieve the goals of greater openness, transparency and freedom of access to technology. These examples illustrate how hackers, as non-state actors, can equally have a significant influence on the substance and implementation of laws and are thus worthy of serious attention and consideration from law and policymakers.

6.1.2 RESOLVING CONFLICTS BY BUILDING ON COMMONALITIES

While the relations and interactions between hacking and law are complex and often tense, given that they essentially share some of the same social goals, it may be possible to lessen or resolve the conflicts between them by building on the values they hold in common. Public authorities have worked with and supported different types of hackers before. The hacking projects and activities of the original computer hackers at MIT were encouraged and funded by the US government (see Section 2.2.1), and a number of countries are promoting the adoption and use of FOSS.¹ As illustrated in the enactment of net neutrality legislation in the Netherlands, hackers and public authorities can align their priorities and goals and work to preserve open and equal access to the internet (see Section 5.2.3.1).

Of course, the ability of hackers and public authorities to resolve some of their differences and work for a common purpose is heavily dependent on their level of trust, understanding and willingness to work with the other. A key consideration in this regard is their general animosity to each other. As explained in Section 5.1.1, the

¹James Andrew Lewis, "Government Open Source Policies" <<https://csis.org/publication/government-open-source-policies-0>> accessed 5 February 2016; see also Robert Hahn, "Government Policy toward Open Source Software: An Overview".

aversion of hackers to public authorities is founded on their anti-establishment spirit and their overall dislike of centralized authorities, hierarchies and bureaucracies. It may be possible though to narrow the gap and bring hackers and public authorities closer together if both sides develop a more tolerant or empathetic view of each other.

With regard to hackers, while it is true that they mistrust public authorities,² they are not completely against the latter. The campaign against electronic voting machines is particularly noteworthy and can shed light on this issue (see Section 5.2.2.2). I was initially perplexed by the apparent contradiction: why were hackers so concerned about the dangers of electronic voting and the importance of preserving the security and integrity of the electoral process, when it ultimately resulted in the election of public officials? If hackers really despised public authority (as most of them claim), would it not have served their purposes better to allow the continued use of the voting machines and then subsequently show the problems with the voting process, and thus call into question the authority of elected public officials? Based on my interviews and observations, I believe that, in the same manner that makers and hacktivists understand law in two different senses (i.e., as restrictive or unjust prescriptions of centralized authorities but also as the foundation or source of fundamental rights and freedom), hackers similarly conceive of public authorities in two distinct ways. The hackers I met mainly see public authorities as embodiments of centralized power and control, but they also consider authorities to be representatives or agents of the demos. While hackers may oppose the former conception of public authorities, they are willing to support the latter notion. By de-emphasizing their concerns about the risks and threats of centralized control and power and seeing authorities as public servants who equally strive to achieve liberal democratic goals, hackers can have a more fair and nuanced view of public authorities.

² Steven Levy, *Hackers* 29.

With this change of perspective, makers and hacktivists would be more willing to constructively engage with state actors if they see themselves not so much as working for or under a centralized authority, but working in common with them to protect or advance democratic values and systems. With regard to public authorities, the following sections explain how, due in part to their better understanding and appreciation of hacker culture, they have started to adopt and implement policies that support hacking.

6.2 Support and reach out to hackers

Given the above findings and the fact that makers and hacktivists hold and share principally the same liberal democratic principles and goals that governments seek to protect and promote and they do not engage in malicious activities or intend to cause damage, it would be more productive if the law and public authorities viewed and treated hackers as co-participants, collaborators or equal partners in the development of technology laws and policies, especially with regard to those laws that particularly affect hacking. Responsible disclosure and open data are two of the most noteworthy examples of hackers and public authorities in the Netherlands constructively working together. These two cases demonstrate how supporting and reaching out to makers and hacktivists is a more practical and useful alternative to dealing with hacking than criminal prosecution.

6.2.1 RESPONSIBLE DISCLOSURE

6.2.1.1 Responsible disclosure rules

Recognizing the difficult and complex nature of computer security, public authorities are beginning to adopt policies that acknowledge and support the crucial roles that hackers play in protecting and improving the security and safety of public and private information

systems and networks.³ In the Netherlands, the Ministry of Security and Justice through the National Cyber Security Centre (NCSC) issued a “Policy for arriving at a practice for Responsible Disclosure” in early 2013.⁴ The central goal of the responsible disclosure guideline is to establish a policy framework that clarifies the roles and responsibilities of hackers and owners of computer systems and encourages them to adhere to practices and processes for the expedient and efficient discovery, disclosure and rectification of security vulnerabilities.⁵ The responsible disclosure guideline seeks to accomplish these goals by setting out the basic principles and actions that both the discloser and the system owner must follow or perform.⁶ The guideline, for instance, provides that the system owner is primarily responsible for its security.⁷

Pursuant to the guideline, a discloser of a security vulnerability (who is usually an ethical hacker or security researcher) should report the vulnerability first and “as quickly as is reasonably possible” to the system owner or administrator.⁸ In reporting the vulnerability, the discloser must do so “in a manner that safeguards the confidentiality of the report”.⁹ With regard to the discovery of the vulnerability, the discloser’s actions “must not be disproportionate”.¹⁰ The guideline lists a number of acts that are considered disproportionate or improper, including the discloser “using social engineering”, “building his or her own backdoor”, “using brute force attack to gain access to the system”,¹¹ or “copying, modifying or deleting data on the system”. Under the guideline, rather than copying data to prove that he or she was able

³ See Arjen Kamphuis, “Dining with Assange and Spies”.

⁴ Loek Essers, “Dutch government aims to shape ethical hackers’ disclosure practices”.

⁵ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 5-6; Ministry of Security and Justice, National Cyber Security Centre, “Policy of Public Prosecution Service on ethical hackers in line with Responsible Disclosure guidelines”.

⁶ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

⁷ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7; see also Council Directive 2013/40/EU on attacks against information systems, recital 26.

⁸ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 8; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 36.

⁹ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 8; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 39.

¹⁰ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 8.

¹¹ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 8.

to gain access, the discloser should simply make “a directory listing of the system”.¹²

On their part, system owners and administrators are encouraged to draft and implement their own responsible disclosure policies and make them publicly available and accessible so that hackers and security researchers are aware of what systems and data they can access and test, what techniques they can use, and what procedures they should follow.¹³ Pursuant to the guideline, a system owner’s responsible disclosure policy should also explicitly state whether it would decline “to take legal action where the discloser acts in accordance with the policy”.¹⁴ In addition, when they receive a vulnerability report, system owners should have an “adequate response” and this may entail contacting the discloser to discuss the vulnerability, entering into a contract or agreement with the discloser that sets out how the vulnerability and its disclosure will be handled, and keeping the discloser informed about the progress of the rectification process.¹⁵ Furthermore, in consultation with the discloser, the system owner or administrator must decide if or when the vulnerability is disclosed to the wider security community and the public at large.¹⁶ Under the guideline, the standard term for fixing software vulnerabilities is 60 days, while for hardware it is 6 months.¹⁷ The system owner is also urged to give “the discloser credit for the report, if the discloser so desires” or even “some form of remuneration/recognition” for discovering and disclosing the security vulnerability.¹⁸

The responsible disclosure guideline is compatible with the developing practice of bug bounty programs. Through bug bounty

¹² Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 8.

¹³ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

¹⁴ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

¹⁵ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

¹⁶ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

¹⁷ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

¹⁸ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 7.

programs, companies actively solicit hackers and security researchers to find and report computer bugs and security vulnerabilities in their systems, software and services by publicly offering rewards for such reports and disclosures.¹⁹ The rationale behind bug bounties is founded on a well-known hacker principle dubbed Linus’s Law (named after Linus Torvalds, the creator of Linux), which states that “Given enough eyeballs, all bugs are shallow”.²⁰ Within the information security industry, it is acknowledged that one “can’t rely on automated approaches or occasional consultants. You need a big group with a diverse set of skills constantly probing your system for weakness”.²¹ With bug bounty programs, companies can “tap into the supply of global hackers” and “they are cheaper than hiring full-time security researchers”.²² Within a short amount of time, bug bounty programs have become a widely accepted practice in the information technology industry, and major companies like Google, Microsoft and PayPal now offer gifts, recognition and even significant sums of money to hackers who discover and disclose bugs pursuant to prescribed procedures,²³ which hew closely to the extant responsible disclosure practices of ethical hackers and security researchers.²⁴ Offering bug bounties for security vulnerabilities is also spreading to other industries.²⁵

From a legal and policy perspective, the responsible disclosure guideline is quite noteworthy for a number of reasons. First, it expressly acknowledges that there are ethical hackers and security researchers who are not interested in maliciously accessing or damaging comput-

¹⁹ HackerOne, “Vulnerability Disclosure Guidelines” <<https://hackerone.com/disclosure-guidelines>> accessed 13 August 2015; Cassandra Kirsch, “The Grey Hat Hacker” 397; Ben Popper, “A new breed of startups is helping hackers make millions - legally”.

²⁰ Eric Raymond, *The Cathedral and the Bazaar* 30; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 9.

²¹ Ben Popper, “A new breed of startups is helping hackers make millions - legally”; see also James Conrad, “Seeking help: the important role of ethical hackers”; see also Chris Evans, “Announcing Project Zero”.

²² Ben Popper, “A new breed of startups is helping hackers make millions - legally”; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 49.

²³ Andy Greenberg, “Meet ‘Project Zero,’ Google’s Secret Team of Bug-Hunting Hackers”; *The Bug Bounty List*, <<https://bugcrowd.com/list-of-bug-bounty-programs/>> accessed 13 August 2015; Ben Popper, “A new breed of startups is helping hackers make millions - legally”; HackerOne, “Vulnerability Disclosure Guidelines” (<<https://hackerone.com/disclosure-guidelines>> accessed 13 August 2015; Cassandra Kirsch, “The Grey Hat Hacker” 386 and 397.

²⁴ HackerOne, “Vulnerability Disclosure Guidelines” (<<https://hackerone.com/disclosure-guidelines>> accessed 13 August 2015.

²⁵ Ben Popper, “A new breed of startups is helping hackers make millions - legally”; *The Bug Bounty List*, <<https://bugcrowd.com/list-of-bug-bounty-programs/>> accessed 13 August 2015.

ers but are motivated to “improving the safety of ICT systems by probing vulnerabilities and risks”.²⁶ Their aims are “exposing vulnerabilities in public and government systems to improve system and network security, while promoting advances in technology and consumer protection”.²⁷ Second, the guideline was a result of and based on consultations and open discussions with a number of public and private stakeholders including members of the hacker and computer security communities.²⁸ Third, it emphasizes the importance of a cooperative and collaborative approach that brings together hackers, private organizations and the government to work together as partners on “the common goal of increasing the security of information systems”.²⁹ It is particularly noteworthy how the NCSC has played a pivotal role in serving as an intermediary between hackers and private organizations.³⁰ In one case, when a vulnerability was reported to a company, the company “didn’t act initially” so the discloser “had to ask the NCSC and then they pressured them into a response and then finally they did something about it”.³¹ “In the end, it did help that the NCSC worked with” the discloser “to tell them that this was actually very serious and that they had to do something about it. That helps”.³² Finally, the principles and rules contained in the responsible disclosure guideline are based on and may be considered a codification of the actual and existing customs, practices and processes of security researchers and other hackers involved in computer security.³³

²⁶ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 3 and 5; see also Government of the Netherlands, “Guidelines for responsible disclosure of IT vulnerabilities”; see also Ministry of Security and Justice, National Cyber Security Centre, “Public-Private Cooperation”.

²⁷ Cassandra Kirsch, “The Grey Hat Hacker” 388.

²⁸ Interview with Maker H; Interview with Ethical Hacker A; Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 3 and 5; Government of the Netherlands, “Guidelines for responsible disclosure of IT vulnerabilities”; Ministry of Security and Justice, National Cyber Security Centre, “Public-Private Cooperation”.

²⁹ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 3 and 5; see also Government of the Netherlands, “Guidelines for responsible disclosure of IT vulnerabilities”; see also Ministry of Security and Justice, National Cyber Security Centre, “Public-Private Cooperation”.

³⁰ Interview; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 5 and 49 (on voluntary intermediaries for security vulnerabilities or vulnerability clearinghouses)

³¹ Interview; see also Cassandra Kirsch, “The Grey Hat Hacker” 388.

³² Interview.

³³ Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure” 3 and 5; Government of the Netherlands, “Guidelines for responsible disclosure of IT vulnerabilities”; see Ministry of Security and Justice, National Cyber Security Centre, “Public-Private Cooperation”; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 35-36.

The responsible disclosure guideline manifests a changing attitude of public authorities towards hackers, and is an example of a pragmatic and nuanced regulation that constructively responds to and takes into account some of the technical and social benefits of hacking. But certain issues and limitations remain. The guideline is best characterized as a form of soft law for government actors, organizations and hackers to voluntarily follow. This means that, while the guideline is highly persuasive, it is not in itself legally binding or enforceable.³⁴ Further, it does not create a legal exemption from liability for hackers since even if a system owner's policy expressly provides that "no police report will be filed if the reporter has acted in accordance with the agreements. The independent power of the Public Prosecutor to proceed with the prosecution if the suspicion exists that a crime has been committed will continue to exist".³⁵ As confirmed by the Board of Procurators General, after and in response to the issuance of the NCSC's guideline, "If, in revealing the vulnerability, the person making the report has committed a punishable act, the responsible reporting of the vulnerability does not in any way safeguard him against the police... will instigate a criminal investigation, and/or that legal proceedings may ensue".³⁶ So, even if a system owner has a responsible disclosure policy in place and a discloser has complied with both the general guideline and the specific policy in disclosing the security vulnerability, the Public Prosecution Service may still pursue the matter further as "it may be necessary first to instigate a criminal investigation and to regard the hacker as a suspect" to be able "to discover whether a reporting by a hacker was necessary and proportional under the given circumstances".³⁷ Of course, if it is determined that a discloser acted properly pursuant to the responsible disclosure rules,

³⁴ Government of the Netherlands, "Guidelines for responsible disclosure of IT vulnerabilities"; Board of Procurators General, "Responsible Disclosure (how to deal with 'ethical' hackers?)" (18 March 2013) 2.

³⁵ Government of the Netherlands, "Guidelines for responsible disclosure of IT vulnerabilities"; see also Ministry of Security and Justice, National Cyber Security Centre, "Policy of Public Prosecution Service on ethical hackers in line with Responsible Disclosure guidelines".

³⁶ Board of Procurators General, "Responsible Disclosure (how to deal with 'ethical' hackers?)" (18 March 2013) 1.

³⁷ Board of Procurators General, "Responsible Disclosure (how to deal with 'ethical' hackers?)" (18 March 2013) 2.

the investigation should not lead to prosecution.³⁸

6.2.1.2 Hackers' reactions

As can be expected, the hackers that I met have mixed feelings about the responsible disclosure rules. According to Maker G, "I know people who are in favor of the current rules, I know people who are against them".³⁹ Some hackers believe that the guideline is part of an attempt by public authorities to co-opt or recruit hackers to work for government.⁴⁰ "I think part of the reason is the NCSC is a governmental agency and they started promoting the responsible disclosure procedure", explains Maker J, "I know that this is something that is felt among some of the hackers".⁴¹ In addition to their general distrust of things produced by a centralized authority, hackers' negative opinions about responsible disclosure guideline mostly center on the fact that it does not provide a legal exemption from criminal prosecution. As Hactivist B says, "I think it's is a complete façade. Because, in the end, whether or not you're prosecuted is still up to the public prosecutor".⁴² Maker L recounts, "the Justice Department said, even if you follow those rules we may still want to, we think it's good to prosecute you, we are still allowed to prosecute you".⁴³ Ethical Hacker A further elaborates on their dissatisfaction, "That's why I don't fully agree with the content. It says, well if you're the researcher, you should do this and this and this and this and this and that. And if you do that, we cannot guarantee anything. Yah, ok, so why should I do it in the first place?"⁴⁴ On top of that, "even if the company says, 'Great job, no problem that

³⁸ Board of Procurators General, "Responsible Disclosure (how to deal with 'ethical' hackers?)" (18 March 2013) 1-2; see also Jurriaan de Haan, "The New Dutch Law on Euthanasia" 58, 60, 62, 66 (Interestingly, the responsible disclosure rules for disclosing computer security vulnerabilities bears some similarities with the reporting procedures for euthanasia in the Netherlands. Under Dutch law, a physician who has committed euthanasia will not be prosecuted if, among other requirements, he or she has complied with stated reporting rules. While Dutch law does not deprive the public prosecutor of the right to investigate and prosecute cases of euthanasia (or hacking), as a matter of government policy, it will not do so if the specific reporting rules are observed).

³⁹ Interview with Maker G.

⁴⁰ Interviews.

⁴¹ Interview with Maker J.

⁴² Interview with Hactivist B.

⁴³ Interview with Maker L.

⁴⁴ Interview with Ethical Hacker A.

you did it', the government still can prosecute you without any claim from the company itself".⁴⁵ The perennial threat of prosecution is thus a clear disincentive to complying with the guideline or making a disclosure at all. Reporting security vulnerabilities is very risky because "you are making yourself very vulnerable because you're saying, yes I hacked your organization and I found this problem".⁴⁶ Another issue with the responsible disclosure guideline is that, for the rules to actually apply, system owners must put the rules into effect by creating their own responsible disclosure policies. Maker H explains, "So if you don't have any procedures in your organization and someone comes along and says 'I have this', they would adhere to the strictest responsible disclosure that are applied elsewhere but nonetheless are not [free from liability]. And then it says, by and large, even when you have followed these rules we still may be able to prosecute you".⁴⁷

Aside from the lack of an express legal exemption from prosecution in the responsible disclosure rules, several hackers also took issue with the very use of the term "responsible disclosure". Maker J states that the term is "a bit ill-chosen... because responsible disclosure puts the act with the hacker, with the discloser, saying that it is his responsibility to act responsibly".⁴⁸ Hactivist D agrees, "As far as I know, now the rules are a little bit lopsided. They do protect the companies quite a bit, not so much the person exposing the vulnerability".⁴⁹ And to make matters worse, "the biggest problem is there's been a bad track record with companies not dealing... well with people saying what they are doing wrong" and who expose security vulnerabilities.⁵⁰ "I think it's not really clear how, who takes responsibility for" the security issues that were discovered, says Ethical Hacker B.⁵¹ Moreover,

⁴⁵ Interview with Maker L.

⁴⁶ Interview.

⁴⁷ Interview with Maker H.

⁴⁸ Interview with Maker J.

⁴⁹ Interview with Hactivist D.

⁵⁰ Interview with Hactivist D.

⁵¹ Interview with Ethical Hacker B.

Hactivists B believes, “I think it trivializes responsible disclosure” because “what is and what isn’t responsible isn’t in every case an individual ethical dilemma, which cannot be formalized in like a rule or one policy”.⁵² In Hactivists F’s view, “To me this is about the individual’s responsible disclosure”.⁵³ Hactivist E also has concerns about how public authorities may interpret the meaning of responsible,

I do find the name “responsible disclosure” a bit troublesome: it seems to imply that any disclosure that does not comply with it is irresponsible. Probably disclosures have occurred that NCSC would consider to be irresponsible and that I would consider to be acceptable [or] reasonable.⁵⁴

Maker J prefers the term “coordinated disclosure” because “it’s actually more of a coordinated process, where they both have to” work together to resolve the security issue.⁵⁵

Despite these issues and concerns, many hackers that I spoke to have a relatively positive opinion of the responsible disclosure rules.⁵⁶ Maker J thinks the guideline is “very good”,⁵⁷ and Maker D says, “I like it. It’s good. It’s change”.⁵⁸ Maker H is critical yet pragmatic about the rules, “I would say that I’m not happy with the responsible disclosure rules as they are. However in practice they seem to be working reasonably well”.⁵⁹ Ethical Hacker A holds a similar view, “I do not fully agree with the content but I’m really happy with the process.... The content can be better but the process of addressing the issue is ok”.⁶⁰ Like other hackers, Hactivist D generally considers the guideline to be a step in the right direction because “in principle, of course, it’s good to protect people who try to do good by exposing vulnerabilities”.⁶¹

⁵² Interview with Hactivist B.

⁵³ Interview with Hactivist F.

⁵⁴ Interview with Hactivist E.

⁵⁵ Interview with Maker J.

⁵⁶ Interview with, among others, Maker D, Maker L and Ethical Hacker B.

⁵⁷ Interview with Maker J.

⁵⁸ Interview with Maker D.

⁵⁹ Interview with Maker H.

⁶⁰ Interview with Ethical Hacker A.

⁶¹ Interview with Hactivist D.

For Hactivist E, “I consider the guideline to be a good development because it may trigger organizations into establishing a somewhat hacker-friendly disclosure policy”.⁶² Hactivist E further explains how the guideline “helps clarify communications between organizations and those who want to report vulnerabilities. Hopefully, organizations will embrace unsolicited vulnerability reports rather than fear or fight them: then we’re all be better off in the end”.⁶³ Hactivist F points out though that aside from being “long overdue”, the adoption of the guideline is “simple... not rocket science”.⁶⁴ “I have a hard time thinking of how if you’re a sane and sensible person you would come to anywhere else than sort of a responsible disclosure measure”, explains Hactivist F.⁶⁵

6.2.1.3 Changing attitudes, changing laws

For all of its above benefits and shortcomings, what is truly remarkable about the responsible disclosure guideline is that it codifies or formalizes existing customs and practices of hackers and security researchers. Rather than being determined or imposed from the top-down, the responsible disclosure rules were developed from the bottom-up and are based on the social norms and values of the relevant community or society – in this case, hackers.⁶⁶ Ethical Hacker B confirms, “to be fair, before the law was there, we did it in this way. The law actually describes exactly what we do”.⁶⁷ “We always did that.... They [the NCSC] kind of basically wrote down what we were already doing for years. So yeah, I’m totally happy with” this development.⁶⁸ The procedures and processes prescribed by the guideline are not new to hackers. Ethical Hacker A recounts, “we had the discussions”,⁶⁹

⁶² Interview with Hactivist E.

⁶³ Interview with Hactivist E.

⁶⁴ Interview with Hactivist F.

⁶⁵ Interview with Hactivist F.

⁶⁶ See Amitai Etzioni, “Social norms: Internalization, Persuasion, and History” 159.

⁶⁷ Interview with Ethical Hacker B.

⁶⁸ Interview with Ethical Hacker B.

⁶⁹ Interview with Ethical Hacker A.

if you were interested at the time. This type of discussions started in the '90s with Microsoft, for example. With the bugs, and what should you do, should you do full disclosure or not. And that was a 1990s discussion". "Most people... I know they respect at least the part of informing the target system or the company that runs the target system first. Wait for their response and do something", explains Ethical Hacker A, "As long as the process of informing someone, giving them a reasonable amount of time to fix it and then disclosing. As long as that process is followed I'm comfortable with that".⁷⁰

What also makes the responsible disclosure rules exceptional is that they exhibit a changing response of the law to hacking. Instead of attempting to restrict or control, public authorities and private companies are trying to constructively support and reach out to hackers. The benefit of having a formal responsible disclosure guideline is that "you can show" system owners that "on a government level they're also working on it. And if they're already working on it on a government level, well then it's well accepted".⁷¹ Maker H notes how "by and large, people in the industries affected feel, yes we should deal with that, not bring out the full brunt of the law and try to find a middle ground".⁷² The change of attitude is taking place among public authorities as well. Maker J relates, "I've had discussions and I think we're seeing now that judges are looking at these kind of things... If you follow the responsible disclosure guidelines they will take you seriously and they see this as you acting responsibly".⁷³ Even the Board of Procurators General expresses the opinion that Dutch law "does not provide a specific defense for a hacker who is acting out of ideological or ethical motives. Although the law does not provide for it, this does not mean that 'ethical' motives cannot play any role in assessing the criminality of the

⁷⁰ Interview with Ethical Hacker A.

⁷¹ Interview with Ethical Hacker A.

⁷² Interview with Maker H.

⁷³ Interview with Maker J.

perpetrator's actions".⁷⁴

The responsible disclosure rules are a significant step in the right direction and other countries should adopt similar rules. However, as Ethical Hacker B remarks, "I do like that it is changing, but I think we're not there" yet.⁷⁵ It is my position that the responsible disclosure rules can still be improved by either: including an express legal exemption for security research in computer crime or other relevant laws;⁷⁶ or getting a court or another adjudicatory body to render a ruling and establish a precedent or jurisprudence that no crime is committed and no liability should attach when activities are done pursuant to the responsible disclosure rules. With regard to the first proposal, I am convinced that this legislative change of granting a legal exemption for security research, while useful from the perspective of the expressive function of law,⁷⁷ will take a lot of time and effort to implement and may not even be necessary. It should be recalled that "without right" is an essential requisite of each of the first four types of computer security crimes discussed in Section 4.2. It is my position that if system owners have responsible disclosure policies that explicitly solicit or permit the public (including hackers) to test their systems (e.g., through bug bounty programs),⁷⁸ then this amounts to their express consent or authorization to hackers to explore and hack their systems.⁷⁹ Since such access and use are with right or permission, an essential element of the crime is lacking and there would be no legal ground for any criminal prosecution. Furthermore, it behooves Dutch public prosecutors, especially in light of their prosecutorial discretion,⁸⁰ to refrain from commencing or pursuing any investigation

⁷⁴ Board of Procurators General, "Responsible Disclosure (how to deal with 'ethical' hackers?)" (18 March 2013) 1.

⁷⁵ Interview with Ethical Hacker B.

⁷⁶ See Derek Bambauer and Oliver Day, "The Hacker's Aegis" 5 and 40; see also Convention on Cybercrime, art 6 (2).

⁷⁷ See Cass Sunstein, "On the Expressive Function of Law".

⁷⁸ See HackerOne, "Vulnerability Disclosure Guidelines" (<https://hackerone.com/disclosure-guidelines> accessed 13 August 2015; see Ben Popper, "A new breed of startups is helping hackers make millions - legally"; see "The Bug Bounty List", <<https://bugcrowd.com/list-of-bug-bounty-programs/>> accessed 13 August 2015.

⁷⁹ Cassandra Kirsch, "The Grey Hat Hacker" 398.

⁸⁰ See Bert-Jaap Koops, "Cybercrime Legislation in the Netherlands" 3 (on prosecutorial discretion)

against a discloser or hacker who has complied with the responsible disclosure rules because, absent a complaint from the system owner or other evidence that such consent was subsequently withdrawn, no crime has *prima facie* been committed since such access and use are presumptively lawful based on the express consent or authorization given by the system owners in their responsible disclosure policies.⁸¹ The second proposal can be promptly realized if a relevant court or judicial body agrees with the above legal reasoning and interpretation and formally enters a judgment stating that no legal liability attaches if a person has complied with the responsible disclosure rules. A more expedient solution would be to include in a Guideline or Directive of the Public Prosecutor a principle or rule that no criminal investigation or prosecution should be undertaken if a discloser has complied with the system owner's responsible disclosure policy since such access is authorized.

6.2.2 OPEN DATA

6.2.2.1 Policies and initiatives

Open data policies and initiatives are another notable example of the law and public authorities productively reaching out to and embracing hacker culture. An open data policy is normally enacted through a legislative or policy measure, initiative or program of a national, regional or local state body.⁸² The European Commission, for instance, amended the PSI Directive⁸³ to encourage the re-use of public data and make laws and policies across Europe more amendable to public access and innovative uses of such data in light of new and emerging technologies.⁸⁴ The Commission even adopted a Decision

⁸¹ See Derek Bambauer and Oliver Day, "The Hacker's Aegis" 40.

⁸² Noor Huijboom and Tijds Van den Broek, "Open data: an international comparison of strategies" 10.

⁸³ Directive 2013/37/EU of the European Parliament and of the Council amending Directive 2003/98/EC on the re-use of public sector information; see also Directive 2003/98/EC of the European Parliament and the Council on the re-use of public sector information.

⁸⁴ Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information; Communication on Open data: An engine for innovation, growth and transparent governance 6-8; see also European Commission, "Guidelines on recommended standard licences, datasets and charging for the reuse of documents" (2014/C 240/01).

on the Re-use of Commission Information covering its own data and how to make it as widely accessible and reusable as possible.⁸⁵ There are a number of countries that have open data policies.⁸⁶ The United States and the United Kingdom have publicized their open data strategies.⁸⁷ In Europe, the Netherlands, France and Italy have established online portals for public data.⁸⁸ As Maker B recounts, “The notion of open data is very old, but it started to get public awareness when Tim Berners-Lee had a TED talk about it” and “had a plea for opening up data from governments”.⁸⁹ Maker B continues, “in the Netherlands... people started to work with it” as well.⁹⁰

The idea of making existing public data freely available to ordinary citizens and users to re-use and build on has captured the interest of many state actors because of the potential political, social and economic benefits.⁹¹ Policy makers wish to support open data because it may produce economic growth, improve social welfare, and lead to scientific and technical advancements.⁹² Governments are further motivated to promote open data because, by being or appearing to be more inclusive and transparent, it may improve their own administrative operations and their relationships with their citizens.⁹³ As the European Commission explains, “Beyond fuelling the innovation and creativity that stimulate economic growth, open public data also empowers citizens, thereby enhancing participatory democracy and promoting transparent, accountable and more efficient government”.⁹⁴ Open data policies are generally embodied in or carried out through

⁸⁵ Commission Decision of 12 December 2011 on the reuse of Commission documents (2011/833/EU).

⁸⁶ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 2-3.

⁸⁷ Data.gov <<http://www.data.gov/>> accessed 21 August 2013; Data.gov.uk <<http://data.gov.uk/about-us>> accessed 21 August 2013.

⁸⁸ Data.overheid.nl <<https://data.overheid.nl/>> accessed 21 August 2013; Data.gouv.fr <<http://www.data.gouv.fr/>> accessed 21 August 2013; “Open data services” <<http://www.dati.piemonte.it/>> accessed 21 August 2013; “Publicdata.eu” <<http://publicdata.eu/>> accessed 21 August 2013.

⁸⁹ Interview with Maker B.

⁹⁰ Interview with Maker B.

⁹¹ Communication on Open data: An engine for innovation, growth and transparent governance 11; Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information 2-3.

⁹² Communication on Open data: An engine for innovation, growth and transparent governance 3-4.

⁹³ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 4.

⁹⁴ Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information 3; Communication on Open data: An engine for innovation, growth and transparent governance 4.

four types of measures, namely: “(a) education and training, (b) voluntary approaches, (c) economic instruments and (d) legislation and control”.⁹⁵ As Huijboom and Van den Broek explain, education and training programs can involve knowledge exchange platforms, guidelines, and conferences, sessions and workshops.⁹⁶ Voluntary approaches may consist of overall strategies and programs, general recommendations, and public voluntary schemes; while economic instruments include competitions, app contests and camps (e.g., hackathons), and financing of open data portals.⁹⁷ Finally, open data legislation or regulation can take the form of public sector information laws, freedom of information acts, and technical standards and monitoring.⁹⁸

While public authorities visibly champion open data, the main “drivers lie predominantly outside government.... Important drivers for open data policy are for instance citizen pressure, market initiatives, emerging technologies and the ideas of thought leaders”.⁹⁹ In contrast, the primary obstacles to open data can be found within governments themselves such as “the closed culture, limited quality of data, lack of standardization and existing charging models”.¹⁰⁰ These general observations are evident as well in the Dutch experience of open data. “On the top, the Dutch government, and the city council, and the mayor, and everybody is happy with open data. They say, ‘Yes, we have to do it,’” narrates Maker B, “But then there’s this middle layer in organizations. They are trained to keep data away from people, to close it in dossiers”.¹⁰¹ Maker L relays the experience of getting access to public data: the data is sort of available “but it’s not like they have a big website: here is our open data, here’s an API, get it out of there, and

⁹⁵ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 5.

⁹⁶ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 5-6.

⁹⁷ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 5-6.

⁹⁸ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 5-6.

⁹⁹ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 9.

¹⁰⁰ Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 9; see Anneke Zuiderwijk and others, “Socio-technical Impediments of Open Data”; see Commission Staff Working Paper Executive Summary of the Impact Assessment accompany the document Proposal for a Directive amending Directive 2003/98/EC on the re-use of public sector information 2-3; see Ton Zijlstra, “The State of Open Data in Europe - Achievements and Challenges” <http://www.zijlstra.org/blog/2013/02/the-state-of-open-data-in-europe-achievements-and-challenges/> accessed 21 August 2013.

¹⁰¹ Interview with Maker B.

those kinds of things”.¹⁰² And, “if you want to have some more [data], you can ask them”.¹⁰³ So, while public data is technically available, it is not easily accessible by the public. As Maker L says, “There is a lot of open data, but it needs to be used. The people need to be able to find it, and I don’t think they promoted it enough to let people use it”.¹⁰⁴ It appears then that, for open data to really succeed, public authorities themselves need to be more open, transparent and willing to collaborate with others. “To get really good open data it requires a change in practice of the work of a lot of people” in government, argues Maker B.¹⁰⁵ The impediments then to open data are primarily “cultural because the technical... can be solved”.¹⁰⁶ Of course, the systems for accessing and using such public data must themselves promote the principles of openness, transparency and freedom of access. As Maker L says, “others have nice sites where they published everything.... you could download, easy to use”.¹⁰⁷ Maker L continues, “I think if they really want to have open data then they should make it more a priority and promote it more”.¹⁰⁸

6.2.2.2 Hackathons

Among the many types of open data projects and initiatives, open data hackathons are especially noteworthy because, aside from their growing popularity, they recognize and manifest the importance of free and open access to and use of information as a matter of public policy. A hackathon, which is portmanteau of the words “hacking” and “marathon”, is defined as a “periodic event where programmers get together at some venue to collaboratively create a new application or software system within a few hours or a few days”.¹⁰⁹ Companies like

¹⁰² Interview with Maker L.

¹⁰³ Interview with Maker L.

¹⁰⁴ Interview with Maker L.

¹⁰⁵ Interview with Maker B.

¹⁰⁶ Interview with Maker B.

¹⁰⁷ Interview with Maker L.

¹⁰⁸ Interview with Maker L.

¹⁰⁹ “Hackathon”, Computer Desktop Encyclopedia <http://lookup.computerlanguage.com/host_app/search?cid=C999999&dcf=6861636b6174686f6c.htm> accessed 20 August 2013.

Facebook regularly organize hackathons among its employees to spur the development of new technologies and applications.¹¹⁰ Open data hackathons are a type of hackathon where public sector information (PSI) (i.e., “information produced, collected or paid for by public organisations”) is re-used to produce new products and services for commercial and non-commercial use.¹¹¹ These hackathons are conducted under the auspices of governments’ open data policies that encourage the organization of “events to award innovative service creation based on public data”.¹¹² The main goal of hackathons is the creation of new applications and technical innovations that produce “innovation, growth and transparency” in society, the economy, and government, respectively.¹¹³ As Maker D explains, a hackathon is a convenient “way of getting a lot of people together doing technological activities. It’s very good”.¹¹⁴ According to Maker B, hackers “are totally happy with the idea of open data. They want to do things with it”.¹¹⁵ Maker B continues, “the power of real open data is that you make applications and networks... with it” such as “social related apps and also smart embedded electronics”.¹¹⁶

Open data hackathons are taking place all over the world and they are among the most visible and well-publicized activities concerning open data.¹¹⁷ They generate much interest and attention from both the public and private sectors because the applications and technologies developed at these events can have significant socio-economic impacts. Examples of successful software and services that were developed during hackathons include Taarifa (an open source web platform

¹¹⁰ Steven Levy, *Hackers 475*; Mark Zuckerberg, “The Hacker Way”.

¹¹¹ Communication on Open data: An engine for innovation, growth and transparent governance 2, 8 and 11; see also Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information 3.

¹¹² Noor Huijboom and Tijs Van den Broek, “Open data: an international comparison of strategies” 6.

¹¹³ Communication on Open data: An engine for innovation, growth and transparent governance 11; Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information 2-3.

¹¹⁴ Interview with Maker D.

¹¹⁵ Interview with Maker B.

¹¹⁶ Interview with Maker B.

¹¹⁷ See “Open Data Day 2013” <http://wiki.opendataday.org/2013/City_Events> accessed 21 August 2013; see “Europeana hackathons” <<http://pro.europeana.eu/web/guest/hackathon-prototypes>> accessed 21 August 2013.

for finding working water points in Africa),¹¹⁸ GroupMe (a group text messaging app that was acquired by Skype for US\$80M),¹¹⁹ Appetas (a website builder for restaurants that was purchased by Google),¹²⁰ and Easy Taxi (a taxi hailing mobile app).¹²¹ In the Netherlands, open data hackathons have been held in various cities with the support of local governments and private individuals and groups.¹²² During the nationwide activities of the Open Innovatie Festival 2012 (Open Innovation Festival 2012) in the Netherlands, I participated in a hackathon in Leeuwarden.¹²³ Quite interestingly, the national theme for that year was “mutiny” and, quoting Steve Jobs, their motto was “It’s more fun to be a pirate than to join the Navy”.¹²⁴ Dubbed “Kickstart058”, the hackathon was jointly organized by the municipal council and the local hackerspace Frack.¹²⁵ The 24-hour “hack the government” event was aimed at finding “new ways of working together... between government, knowledge institutions, citizens and entrepreneurs”.¹²⁶ While the organizers of the hackathon sought the development of apps that produced “social and economic value”, greater emphasis and preference seem to have been placed on innovations with commercial application or economic impact.¹²⁷ The organizers specifically sought to stimulate “new business opportunities” through the creation of new applications and services based on public data provided by the municipality of Leeuwarden and the province of Friesland.¹²⁸ It is quite notable that one of the stated criteria for selecting the winner of the hackathon was

¹¹⁸ Taarifa, <<http://taarifa.org/>> accessed on 15 January 2016; see also Taarifa, <<https://taarifa.wordpress.com/>> accessed on 15 January 2016.

¹¹⁹ GroupMe, <<https://groupme.com/>> accessed on 15 January 2016; Spencer Ante, “Skype to Acquire Start-Up GroupMe” <<http://www.wsj.com/articles/SB10001424053111903327904576522964260277734>> accessed on 15 January 2016.

¹²⁰ Appetas, <<http://www.appetas.com/>> accessed on 15 January 2016; see also Vinnie Mancuso, “5 Hackathon Success Stories” <<https://finance.yahoo.com/news/5-hackathon-success-stories-131311777.html>> accessed on 15 January 2016.

¹²¹ Easy Taxi, <<http://www.easytaxi.com/>> accessed on 15 January 2016.

¹²² Interview with Maker D; see also Open Cultuur Data <<http://www.opencultuurdata.nl/>> accessed 21 August 2013; see also “Open data NEXT” <<https://data.overheid.nl/english>> accessed 21 August 2013.

¹²³ Open Innovatie Festival 2012 <<http://www.oif2012.nl/>> and <<http://www.oif2012.nl/oif058/>> accessed 21 August 2013.

¹²⁴ Open Innovatie Festival 2012 <<http://www.oif2012.nl/>> and <<http://www.oif2012.nl/oif058/>> accessed 21 August 2013.

¹²⁵ “Kickstart Leeuwarden” <http://frack.nl/wiki/Kickstart_Leeuwarden> accessed 19 November 2012; Frack <<http://frack.nl/>> accessed 21 August 2013.

¹²⁶ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%20kickstart058>> accessed 19 November 2012.

¹²⁷ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%20kickstart058>> accessed 19 November 2012; “Kickstart Leeuwarden” <http://frack.nl/wiki/Kickstart_Leeuwarden> accessed 19 November 2012.

¹²⁸ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%20kickstart058>> accessed 19 November 2012; “Kickstart Leeuwarden” <http://frack.nl/wiki/Kickstart_Leeuwarden> accessed 19 November 2012.

that “the application can be made profitable. This would require a business model that is clear and an idea that is viable”.¹²⁹ Participants could access and re-use data sources such as, among others, population figures, social services information, housing income, migration statistics, economy figures, unemployment numbers, spatial plans and city maps.¹³⁰ It is worth noting that while the municipality was very open to giving access to its data and had technical people on hand to help assist participants, the teams had some difficulties fully working with or using the data since the latter were saved in file formats or stored in databases that were not as easily accessible, interoperable or extractable.

As with most hackathons, there was no fee to enter the event and it was open to the public.¹³¹ “Officials, entrepreneurs, artists, students and professionals” were especially encouraged to participate.¹³² Even people with no technical expertise or background were enjoined to take part since the conceptualization, marketing and distribution a new application or product would require non-technical skills as well.¹³³ During the hackathon, government employees, hackers, students and designers formed and worked in teams on various projects such as an augmented reality mobile app that showed cultural and historical information as the user walked around the municipality, a web-based crowd funding service for community projects, and a housing website. During the 24 hours that the teams worked on their projects, the atmosphere was convivial, although some hackers felt that some of their team members, particularly those who work for the municipality, were too critical and not open to suggestions. In the end, the augmented reality app that was originally proposed and developed by local design students was awarded the prize, which included the allocation

¹²⁹ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%2Fkickstart058>> accessed 19 November 2012; “Kickstart Leeuwarden” <http://frack.nl/wiki/Kickstart_Leeuwarden> accessed 19 November 2012.

¹³⁰ “Kickstart Leeuwarden” <http://frack.nl/wiki/Kickstart_Leeuwarden> accessed 19 November 2012.

¹³¹ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%2Fkickstart058>> accessed 19 November 2012.

¹³² “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%2Fkickstart058>> accessed 19 November 2012.

¹³³ “Hackathon ‘Kickstart058’” <<http://oif058.fikket.com/event/hackathon%2Fkickstart058>> accessed 19 November 2012.

of development time for the app from a local technology company.

Despite the numerous hackathons being held throughout the Netherlands, it is true that they have yet to produce a truly novel “killer application” that can produce significant or far-reaching socio-economic effects that are much sought after. Maker B admits that “there’s no big breakthrough, I think, resulting from the open data movement” in the Netherlands.¹³⁴ Maker D agrees, “Yeah, there are a lot of people who are still inspired, still doing good stuff, but not a really killer app”.¹³⁵ Of course, the applications and technologies developed during open data hackathons are nonetheless quite useful for their intended audiences and offer much value in their own right. Nevertheless, the lack of a killer app and the difficulties of inculcating the values of freedom of access, openness and transparency in government have led to a perceived decline in the interest in open data. Among makers, there is a sentiment that the hype around open data has already peaked and the government’s support for open data has started to wane. “I think there was a momentum at one point but the momentum went away a bit”, relates Maker L, “In the end, [it] slowed down and died a bit”.¹³⁶ For makers, taking part in hackathons “was very interesting. We learned a lot about it. We had a nice amount of fun... but there was not a lot of follow up” from government.¹³⁷ Maker B observes that “there’s a lot of progress in different directions and different fields but it is crawling and it’s spread... it’s not one big breakthrough”.¹³⁸

Notwithstanding these problems and setbacks, open data policies and hackathons attest to a shift in technology law and policy whereby public authorities seek not only to promote greater availability of and access to public data, but also to openly support innovative and creative uses of that data. This change of policy and attitude to-

¹³⁴ Interview with Maker B.

¹³⁵ Interview with Maker D.

¹³⁶ Interview with Maker L.

¹³⁷ Interview.

¹³⁸ Interview with Maker B.

wards hackers is all the more significant given that the public visibility of hackathons provides hacking with a sense of acceptance and legitimacy. Furthermore, open data hackathons illustrate how public authorities, hackers and ordinary citizens can come together to produce techno-social change and innovation.¹³⁹

6.3 Change and improve the law

Responsible disclosure rules and open data hackathons are indicators of a discernable change in direction and orientation of technology laws and policies whereby public authorities have begun to see the benefits and desirability of welcoming and even embracing hacker culture and constructively collaborating with hackers. However, in order to genuinely and meaningfully improve the laws concerning hacking and to encourage hacking's creativity and innovation, existing computer crime, intellectual property and other relevant laws must be changed bearing in mind the attendant practices, norms and values of hackers. As set out below, the proposed legal reforms can be achieved through legislative amendments, judicial rulings, and/or executive interpretations and implementations.

6.3.1 COMPUTER CRIME LAWS

6.3.1.1 Hacking as a legitimate and common activity

Improving the treatment of hackers under the law requires a change in how hacking is viewed and dealt with by public authorities. As previously mentioned in Section 4.2.3.6, computer crime laws provide that "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practic-

¹³⁹ See Publicdata.eu <<http://publicdata.eu/related>> accessed 21 August 2013; see MapLight <<http://maplight.org/about>> accessed by 21 August 2013.

es should not be criminalised”.¹⁴⁰ This means that social norms and customary practices in the field of information and communications technology should be taken into account when determining whether an activity is legitimate and common.

From the early computer hackers at MIT to present-day makers and hacktivists,¹⁴¹ it is evident that hacking, which is basically the creative and innovative use of technology, has always been present and is an integral part of the creation and development of computers and information technologies and networks. There are compelling grounds to argue that hacking is the quintessential activity or practice in the fields of computing and information technology. Verily, is there any other activity or practice that is as singular and inherent in the design and use of computers and information networks as hacking? While this claim may sound radical at first, it is borne out by the symbiotic histories of hacking and technological advances. Hackers and hacking have been the driving force behind the invention or subsequent innovation of many world-changing technologies such as personal computers, open source and commercial software, computer gaming, the internet, the World Wide Web, encryption, peer-to-peer file sharing, social networking sites, personal 3D printers, to name a few.¹⁴² When it comes to information technology, hacking is neither aberrant nor illicit because, in actuality, it embodies the very essence of technical creativity and innovation. Hacking is a creative rather than a criminal activity since it is normally carried out for useful purposes and without any malice or intent to cause damage. For a practice that has produced so much socio-technical breakthroughs, how can it be viewed as anything but a legitimate and common activity? The creative and unexpected uses of technology, which hacking epitomizes, are socially accepted

¹⁴⁰ Explanatory Report to the Convention on Cybercrime, para 38.

¹⁴¹ See Chapter 2 (on the history of hacking and the different types of hackers).

¹⁴² Steve Wozniak, creator of the Apple II (see Steven Levy, *Hackers* 249), Richard Stallman, founder of the Free Software Foundation (see Sam Williams, *Free As In Freedom* 8), Linus Torvalds, developer of Linux (see Linus Torvalds and David

and expected not just among hackers but also the growing number of users who desire to have greater freedom and control over their technologies. Hacking definitely resides at the very heart of technological innovation and is in itself an unmistakably legitimate and common practice.

It should be borne in mind that, like any element or aspect of culture, technical practices and usages in the field of information and communications technology are never static and they are constantly developing, changing and evolving. It may be said that given the premium that both hackers and the information technology industry place on continually producing innovation and furthering technical advances, technological activities and practices intrinsically demand the pushing of boundaries (whether they be technical, legal or social) in order to create something new, different or surprising. Being innovative necessitates the freedom to use technology in unusual, unexpected and creative ways, which is what hacking is all about. Hacking and the creative-destructive dynamic that it engenders are therefore, not only legitimate and common, but also essential for technological and social progress. Hacking projects and activities that are committed without malice or intent to cause damage should be supported rather than proscribed by technology law and policy.

6.3.1.2 Essential requirement of criminal intent

Beyond the shadow of a doubt, the most consequential improvement to hacking-related laws would be the reform of computer crime laws, particularly in relation to illegal access and other computer

Diamond, Just for Fun 122), Bill Gates, who helped create the software industry (see Robert Cringley, *Accidental Empires* 9), John Carmack, founder of Id Software (see Henry Lowood, "Players as Innovators in the Making of Machinima" 170), Vint Cerf and other internet pioneers (see Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late* 158, 179 and 190), Tim Berners-Lee, inventor of the World Wide Web (see Tim Berners-Lee, "Aaron is dead" W3C mailing list), Shawn Fanning, creator of Napster (see Steve O'Hear, "Inside The Billion-Dollar Hacker Club" <<http://techcrunch.com/2014/03/02/w00w00/>> accessed on 10 October 2015), Bram Cohen, developer of the BitTorrent protocol (see Clive Thompson, "The BitTorrent Effect"), Mark Zuckerberg, founder of Facebook (Mark Zuckerberg, "The Hacker Way"), and Adrian Bowyer, inventor of the RepRap open source 3D printer (see RepRap, "About" <<http://reprap.org/wiki/About>> accessed on 2 October 2015) are considered or view themselves as hackers.

security crimes. As discussed at length in Section 4.2, computer security crimes are overly broad and vague and the law over-criminalizes hacking. The law fails to properly distinguish between malicious attacks and attackers and the innovative albeit disruptive activities of hackers. The most sensible approach to improve computer crime laws is to include the subjective criteria of malice, dishonest intent, or intent to cause damage as essential elements of the crimes of illegal access,¹⁴³ illegal interception and possibly even other computer security crimes. Including these additional requisites for the commission of computer security crimes would not require a dramatic change in the law because the Convention on Cybercrime already allows state parties to “require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent” for illegal access and, likewise, “require that the offence be committed with dishonest intent” with respect to illegal interception. The Netherlands and other signatory countries to the Convention can thus simply incorporate the requirement of malicious, dishonest or criminal intent into their domestic computer crime laws.¹⁴⁴ A few states have already included such additional qualifying circumstances for the crime of illegal access in their national laws. For example, the Slovakian Criminal Code provides that unauthorized access to a computer system must be committed “with the intent to cause damage or any other prejudice to another, or to obtain undue advantage for himself or for another”,¹⁴⁵ while the Brazilian Criminal Code criminalizes “[t]respassing a third party’s computing device... by undue breach of the security mechanism, to obtain, tamper with or destroy data or information without express or tacit consent from the owner of the device or install vulnerabilities to obtain illicit advantage”.¹⁴⁶

¹⁴³ Convention on Cybercrime, arts 2 and 3 (emphasis added).

¹⁴⁴ See also Recommendation No. R (89) 9 on computer-related crime 53 and 61 (other subjective criteria to consider are “dishonest or harmful intentions” or “malicious acts”).

¹⁴⁵ Slovakian Criminal Code, section 247.

¹⁴⁶ Brazilian Criminal Code, art 154-A (emphasis added).

It is worth pointing out that the inclusion of additional qualifying circumstances to computer security crimes is not unheard of. In fact, the amended Cybercrime Directive has made “infringing a security measure” a mandatory requirement for the commission of illegal access in Europe.¹⁴⁷ While this legislative reform is commendable, it may be said that it does not go far enough in resolving the over-criminalization of hacking and the lack of nuance in the application of the illegal access provision to hackers. It is true that the overt acts of placing security measures by the system owner and the infringement of such measures by an attacker makes it quite clear for both sides whether a line has been crossed. A person who defeats or breaches a security measure to gain access to a system cannot claim that the entry or access was done unintentionally. However, as explained in Section 4.4.2, owners and rights holders often protect their information and technologies with security measures and anti-circumvention technologies that prevent ordinary users and hackers from engaging in legitimate forms of access and use such as scientific research, security testing or protecting their privacy.¹⁴⁸ So, ethical hackers who endeavor to audit and improve the security of a system will still be held liable under the amended Directive (unless they have permission from the computer owner for the testing) since infringing a security measure is often a necessary part of good security testing. By not having a subjective criterion like malicious or dishonest intent, the law fails to distinguish between legitimate activities like security research versus malicious cyber attacks. While the amended illegal access provision in the Cybercrime Directive makes it easier to determine the intentionality of an act (i.e., whether the act of access was intentional or not),¹⁴⁹ it stops short of ascertaining the substance and context of the act – whether the actual intention was benign or malicious.¹⁵⁰ The law’s deficiency

¹⁴⁷ Council Directive 2013/40/EU on attacks against information systems, art 3.

¹⁴⁸ See Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5; see Cassandra Kirsch, “The Grey Hat Hacker” 398.

¹⁴⁹ See Cyrus Chung, “The Computer Fraud and Abuse Act” 237.

¹⁵⁰ See Tom Brewster, “US cybercrime law being used to target security researchers”.

then lies in the fact that it invites “prosecutorial attention to technology rather than to the culpability of conduct”,¹⁵¹ and it does not reasonably account “for intent”.¹⁵² Malicious intent and the effects of an act should be the ultimate bases on which to judge whether a particular use or access to information or technology is criminal or not. Otherwise, hacking remains overly criminalized since any infringement of a security measure, regardless of actual intent, is prohibited and penalized.

The introduction of a mens rea requirement or similar subjective criteria is extremely important because it makes computer crime laws more precise and equitable in their application. The problem with the current formulation of computer security crimes is that by not requiring “malicious intent or mens rea” (which is “often required in criminal law”), the law “turns general behaviors” like mere entry or access “into strict liability crimes”.¹⁵³ Principles of fairness and justice dictate that the lawfulness or legitimacy of an act should be judged based on the person’s intent (as evidenced or borne out by his or her overt acts) rather than the mere presence or absence of the system owner’s authorization. Requiring the element of “mens rea or criminal intent” would ensure that the law “does not criminalize the legitimate activities and use of tools needed for independent security research, academic study, and other good-faith activities that serve the public interest and ultimately make the public more safe”.¹⁵⁴ Establishing this higher threshold of culpability for illegal access and other computer security crimes is in line with the goals and rationale of computer crime laws. It bears stressing that the Cybercrime Directive unequivocally states that: “This Directive does not impose criminal liability

¹⁵¹ Joseph Olivenbaum, “Rethinking Federal Computer Crime Legislation” 605.

¹⁵² Tom Brewster, “US cybercrime law being used to target security researchers”.

¹⁵³ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5; see also Oliver Wendell Holmes, Jr., “Privilege, Malice, and Intent”; see also Samantha Jensen, “Why Broad Interpretations of the CFAA Fail” 97; see also Orin Kerr, “Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes” 1667.

¹⁵⁴ Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5.

where the objective criteria of the offense laid down in this Directive are met but the acts are committed without criminal intent”.¹⁵⁵ It is quite clear from this recital, which has a controlling effect on the implementation and interpretation of national computer crime laws in Europe, that mere entry, access to or use of a computer without malicious or criminal intent is not a punishable offense.

As a matter of public policy then, it make sense to argue that no crime is or should be deemed committed unless the act of trespass, access or use of a computer or information system is attended with malice, dishonest intent or intent to cause damage. The illegal access provision of the Cybercrime Directive can be amended as follow:

Member States shall take the necessary measures to ensure that, when committed intentionally and with malice, dishonest intent, or intent to cause damage or obtain data, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.¹⁵⁶

Amending the illegal access provision (and potentially the other computer security crimes) in this way would have a positive impact on hacking. As shown in the previous chapters, the makers and hacktivists that I met are not interested in causing damage to computers and data since they generally view malicious activities as having nothing to do with the essence of hacking, which involves the creative, masterful and communitarian uses of technology.¹⁵⁷ With these proposed amendments, makers and hacktivists would be able to finally raise a formidable legal argument against possible criminal prosecution – that their hacking activities were carried out without malicious, dishonest or criminal intent. Certain quarters may argue that including a mens rea requirement would weaken the effectivity of the computer crime

¹⁵⁵ Council Directive 2013/40/EU on attacks against information systems, recital 17 (emphasis added); see also Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” 5.

¹⁵⁶ See Council Directive 2013/40/EU on attacks against information systems, art 2.

¹⁵⁷ Paul Taylor, “From hackers to hacktivists” 628; Tim Jordan, *Hacking 19*; Sam Williams, “Free As In Freedom” 178; “Cracker”, *The New Hacker’s Dictionary*.

laws since “criminal hackers would simply claim in their defence they were carrying out research”.¹⁵⁸ In practice though, “bona fide research” can be proved or disproved in various ways, including the use of basic police investigation and computer forensics.¹⁵⁹ The fact that it might become less convenient for police and law enforcement agencies to gather evidence and prosecute persons for computer security crimes should not be a ground for failing to improve the law.

6.3.2 INTELLECTUAL PROPERTY LAWS

6.3.2.1 Three-step test as akin to fair use

As discussed at length in Section 4.3.3.6, the Netherlands and many countries in Europe and around the world adhere to a closed list approach to limitations and exceptions to intellectual property rights. This means that, unless a particular access to or use of a protected work or invention falls within a specific, statutorily granted limitation or exception (e.g., private and non-commercial use), such access or use is not permitted under intellectual property laws.¹⁶⁰ Because the limitations and exceptions are contained in a static and exclusive list, the closed list approach does not afford the much needed room for makers and other hackers to push the boundaries, develop new technologies, and discover surprising, creative and innovative uses of creative works. Many of the hackers I spoke to relayed how they refrained from exploring technologies or systems or undertaking projects because their activities were not strictly authorized under the law. In contrast, an open-ended approach such as the fair use doctrine followed in the United States and a few other countries,¹⁶¹ allows intellectual property laws to flexibly adjust and dynamically carve out

¹⁵⁸ Tom Brewster, “US cybercrime law being used to target security researchers”.

¹⁵⁹ See Tom Brewster, “US cybercrime law being used to target security researchers”.

¹⁶⁰ Interviews.

¹⁶¹ See Jonathan Band and Jonathan Gerafi, “The Fair Use/Fair Dealing Handbook” 1; see also Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 623-624.

new limitations and exceptions on a case-by-case basis in light of new socio-technical advances and practices.¹⁶² The closed list approach can be dramatically improved to support the innate creativity and innovativeness of hacking by incorporating or adopting into a state's national law or jurisprudence an open-ended standard (akin to the fair use doctrine) that is founded on the three-step test.

The three-step test provides that limitations and exceptions to intellectual property rights should: (1) apply only “in certain special cases”; (2) “not conflict with a normal exploitation of the work”; and (3) “not unreasonably prejudice the legitimate interests of the author”.¹⁶³ Using the three-step test as an open-ended criteria akin to the fair use doctrine can be readily accomplished especially by European countries since, not only are they signatories to international intellectual property conventions like the Berne Convention and the TRIPS Agreement that already provide for the three-step test,¹⁶⁴ but the test is already part of European law having been included in the Copyright Directive as well as other Directives. As explained by Senftleben, “Given the appearance of the three-step test in several EC Directives,¹⁶⁵ the provision can moreover be regarded as part of the established legal principles of EC law”.¹⁶⁶ Using the three-step test as an operative principle or guideline for determining the legitimacy of new technologies and social practices vis-à-vis intellectual property makes sense because judicial, legislative and other regulatory bodies that have to decide whether a reproduction or use of a protected work or invention is permitted or excepted would inevitably need to refer to or apply the three-step test and consider the “potential, as well as current and ac-

¹⁶² See WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 68; see Martin Senftleben, “The Emerging EC Fair Use Doctrine” 527.

¹⁶³ Berne Convention, art 9(2).

¹⁶⁴ Berne Convention, art 9(2); Agreement on Trade-Related Aspects of Intellectual Property Rights, arts 26 and 30.

¹⁶⁵ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 5(5); Directive 2009/24/EC on the legal protection of computer programs, art 6(3); Directive 96/9/EC on the legal protection of databases, arts 6(3) and art 7(5); Martin Senftleben, “The Emerging EC Fair Use Doctrine” 543; see also Martin Senftleben, “The Emerging EC Fair Use Doctrine” 531-532.

¹⁶⁶ Martin Senftleben, “The Emerging EC Fair Use Doctrine” 543.

tual, uses or modes of extracting value from a work”.¹⁶⁷ As confirmed by the WIPO Standing Committee on Copyright and Related Rights, the three-step test “is consciously framed as an omnibus or umbrella provision that is prospectively applicable to all exceptions to the reproduction right” and other rights as well.¹⁶⁸ As such, it can and should be used to expand the limitations and exceptions to intellectual property rights or create new ones.¹⁶⁹

There have been a number of national courts that have applied the three-step test, not as a restrictive check on the validity of a statutory limitation and exception to copyright,¹⁷⁰ but as “flexible, open-ended criteria” for assessing and determining the extent and scope of intellectual property protection in the context of technological developments and innovative uses and activities.¹⁷¹ In the Netherlands, while “the three-step test has little impact on the Dutch catalogue of statutory exceptions... the Directive inspired a line of decisions that use the three-step test to override the closed Dutch system of precisely-defined user privileges”.¹⁷² For instance, a Dutch court resorted to the three-step test rather than the statutory exceptions to resolve a case on the legitimacy of press reviews.¹⁷³ What is noteworthy about this decision is that the court’s “discussion of non-compliance with the three-step test resembles a U.S. fair use analysis rather than a close inspection of a continental-European statutory limitation”.¹⁷⁴ Similarly in Switzerland, the Supreme Court applied the three-step test to create an exception for a commercial service that provided summaries of news

¹⁶⁷ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 23 and 35; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 32.

¹⁶⁸ Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” 25.

¹⁶⁹ Martin Senfileben, “The Emerging EC Fair Use Doctrine” 551.

¹⁷⁰ See Martin Senfileben, “The Emerging EC Fair Use Doctrine” 529, 531 and 532.

¹⁷¹ Martin Senfileben, “The Emerging EC Fair Use Doctrine” 548; see also Christophe Geiger, Daniel Gervais and Martin Senfileben, “The Three-Step Test Revisited” 616 and 618; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35.

¹⁷² Martin Senfileben, “The Emerging EC Fair Use Doctrine” 530.

¹⁷³ Martin Senfileben, “The Emerging EC Fair Use Doctrine” 530.

¹⁷⁴ Martin Senfileben, “The Emerging EC Fair Use Doctrine” 531.

articles.¹⁷⁵ Outside Europe, the Colombian Supreme Court also used the three-step test to create an exception for format-shifting of content for private and non-commercial purposes.¹⁷⁶ These courts notably applied the three-step in an “enabling sense”¹⁷⁷ so as to broaden or add to the existing limitations and exceptions to intellectual property rights.¹⁷⁸ Cases such as these illustrate how national courts can simply and effectively adopt or use the three-step test to modify or even establish new limitations and exceptions beyond those explicitly provided in national statutes.¹⁷⁹ These examples bear evidence to the fact that the three-step test “can be used to enable limitations and enhance flexibility in copyright” and other intellectual property laws.¹⁸⁰

Besides courts and judges, it makes perfect sense for Dutch and other national lawmakers and regulators to “take full advantage of the flexibility inherent in the three-step test that has already become a cornerstone of EC legislation in the field of copyright limitations” and globally as well.¹⁸¹ Quite interestingly, several countries have incorporated the actual text of the three-step test into their national laws. In Europe, the three-step test is expressly provided for in the laws of Croatia, France, Greece, Portugal and Spain.¹⁸² By having the three-step test embodied in national law, it can be used as a legal basis to further enhance or refine the scope of limitations and exceptions to intellectual property rights.¹⁸³ With the three-step test acting akin to the fair use doctrine, national legislators and courts can “use the three-step test either to make specific lists of exceptions or to create open-ended exceptions”.¹⁸⁴ Moreover, having the test as part of domes-

¹⁷⁵ Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 619-620.

¹⁷⁶ Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 620-621.

¹⁷⁷ Martin Senftleben, “The Emerging EC Fair Use Doctrine” 545-546; see also Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 618.

¹⁷⁸ Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 621.

¹⁷⁹ See Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35 (who argues that this may be the case even “where no such specific exception exists, if permitted under domestic law”).

¹⁸⁰ Martin Senftleben, “The Emerging EC Fair Use Doctrine” 546; see also Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 618.

¹⁸¹ Martin Senftleben, “The Emerging EC Fair Use Doctrine” 551.

¹⁸² Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35.

¹⁸³ Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 582.

¹⁸⁴ Christophe Geiger, Daniel Gervais and Martin Senftleben, “The Three-Step Test Revisited” 622; see also Martin Senftleben, “The Emerging EC Fair Use Doctrine” 542-543.

tic law would permit local “courts to identify new use privileges on the basis of the test’s abstract criteria”.¹⁸⁵ This dynamic interpretation and approach to the three-step test is in accord with international law: “The WIPO Internet Treaties confirmed that the three-step test allows the extension of traditional copyright [limitations and exceptions] into the digital environment and the development of appropriate new [limitations and exceptions]”.¹⁸⁶ Furthermore, “the Agreed Statement concerning Article 10 of WCT confirms that the test is intended to serve as a basis for the further development of existing and the creation of new [limitations and exceptions] in the digital environment”.¹⁸⁷ Quite interestingly, the practice of directly applying the three-step as part of national law is gaining ground.¹⁸⁸ While some countries have adopted an open-ended approach to limitations and exceptions by incorporating the fair use doctrine into their national laws,¹⁸⁹ Australia is quite unique in the way it used the elements of the three-step test to craft a fair use-like provision into its copyright law.¹⁹⁰ According to the Australian lawmakers, the “proposed section 200AB seeks to provide an open-ended exception in line with the US model, and allows courts to determine if other uses should be permitted as exceptions to copyright”.¹⁹¹ It is worth noting that

The three-step test was not only incorporated in the Australian provision... it was a central consideration in preparing this Bill. In addition to being addressed directly to courts in section 200AB, the three-step test was used to justify limitations in the formulation of exceptions.¹⁹²

Regardless of which approach a country ultimately chooses, whether through judicial interpretation, legislative enactment, or both,

¹⁸⁵ Christophe Geiger, Daniel Gervais and Martin Senffleben, “The Three-Step Test Revisited” 582.

¹⁸⁶ Christophe Geiger, Daniel Gervais and Martin Senffleben, “The Three-Step Test Revisited” 625-626.

¹⁸⁷ Christophe Geiger, Daniel Gervais and Martin Senffleben, “The Three-Step Test Revisited” 617.

¹⁸⁸ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 34.

¹⁸⁹ See Jonathan Band and Jonathan Gerofi, “The Fair Use/Fair Dealing Handbook” 1; see Christophe Geiger, Daniel Gervais and Martin Senffleben, “The Three-Step Test Revisited” 623-624.

¹⁹⁰ Australian Copyright Amended Act 2006, section 200AB; see also Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 35 and 36.

¹⁹¹ Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 36.

¹⁹² Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 36.

what is essential is the adoption of a dynamic and open-ended standard for the establishment and development of more reasonable and fair limitations and exceptions to intellectual property rights. Having such a standard in place is necessary in order to permit intellectual property laws and policies to quickly and adequately respond to new technological developments and innovative uses of intellectual creations that are being produced as such a heightened pace today.¹⁹³ This is especially true since “public policy considerations are hardly ever static: they change over time, reflecting the needs and realities of the various countries”.¹⁹⁴ The three-step test is a robust and compelling legal basis for making the system of limitations and exceptions more responsive to techno-social advances because it provides “a flexible framework, within which national legislators enjoy the freedom of safeguarding national limitations and satisfying domestic social, cultural and economic needs”.¹⁹⁵ As Senfleben declares, “the time is ripe to... open up the current restrictive system, [and] offer sufficient breathing space for social, cultural and economic needs, and enable [laws] to keep pace with the rapid development of the Internet” and other technologies.¹⁹⁶ By interpreting and applying the three-step test in this manner, intellectual property laws would be able to improve and adapt to changing technologies and social practices and support rather than impede technical and cultural innovation.

6.3.2.2 Three-step test plus

The three-step test is certainly an excellent foundation on which to build an open-ended, fair use-like standard in countries like the Netherlands, which follow a closed list approach to limitations and exceptions to intellectual property rights. I would further argue though

¹⁹³ See Martin Senfleben, “The Emerging EC Fair Use Doctrine” 540.

¹⁹⁴ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 2.

¹⁹⁵ Martin Senfleben, “The Emerging EC Fair Use Doctrine” 550-551.

¹⁹⁶ Martin Senfleben, “The Emerging EC Fair Use Doctrine” 522 and 539.

that to promote the creative and innovative spirit of hacking and to maintain and preserve the intellectual property balance between the rights of creators vis-à-vis the rights of users, the test can still be enhanced by adding another criterion and make it effectively a three-step test plus.¹⁹⁷ The proposed additional requirement to the three-step test is far from being fanciful and is firmly based on developments in international intellectual property law. Article 30 of the TRIPS Agreement provides for the three-step test in relation to patents:

Members may provide limited exceptions to the exclusive rights conferred by a patent, provided that such exceptions do not unreasonably conflict with a normal exploitation of the patent and do not unreasonably prejudice the legitimate interests of the patent owner, taking account of the legitimate interests of third parties.¹⁹⁸

Article 26(2) of the TRIPS Agreement on industrial designs contains the same additional wording.¹⁹⁹ What is curious about these articles is that, aside from the usual requirements of the three-step test, it includes an extra requirement in the third test that it must take into account “the legitimate interests of third parties”.²⁰⁰ It should be noted that the three-step test as originally worded in the Berne Convention does not contain this last phrase.²⁰¹ According to the WIPO Standing Committee on the Law of Patents, “the term ‘legitimate interest’ must be ‘defined in the way that it is often used in legal discourse – as a normative claim calling for protection of interests that are ‘justifiable’ in the sense that they are supported by relevant public policies or other social norms’”.²⁰²

¹⁹⁷ See Peter Drahos, “Bilateralism in Intellectual Property”; see Susan Sell, “TRIPS-plus free trade agreements and access to medicines” (This term “three-step test plus” is a play on “TRIPS-plus”, which are international or bilateral agreements between states that impose “more extensive protection” for intellectual property that are over and above those provided under the TRIPS Agreement. But in this instance, the plus is used to enable rather than restrict access to and use of intellectual property).

¹⁹⁸ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 30 (emphasis added); but see Agreement on Trade-Related Aspects of Intellectual Property Rights, art 13 (for copyright and related rights).

¹⁹⁹ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 26(2).

²⁰⁰ Agreement on Trade-Related Aspects of Intellectual Property Rights, art 30; see also Berne Convention, art 9(2); see also WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 21.

²⁰¹ Berne Convention, art 9(2).

²⁰² WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 22.

For hackers and the general public, a three-step test plus provision is momentous because, not only does it promote the intellectual property balance, but, for the first time, the rights and interests of users and the public (including hackers) who make up the other side of the balance are expressly acknowledged in the letter of the law. As originally worded, the three-step test is arguably oriented or leans towards the side of authors and creators. It may be said that the test favors authors and creators because their rights and interests are the bases on which to determine whether an access or use by others is permitted or excepted under the law. The three-step test plus provision is of great consequence and import because, by including the additional requirement, the test is finally properly balanced since it must consider the interests of all the parties involved: not just authors, creators and rights holders, but also users, consumers, technology developers, and the general public. The three-step test plus provision is all the more significant because it expresses and embodies the principle of the intellectual property balance in a legally actionable form. Policy statements about the intellectual property balance and the need to preserve the public's right to access and use intellectual creations are normally found in the preamble of the law or its explanatory memoranda and they do not make it to the operative text or body of the law. By including an express statement recognizing the rights of users and third parties in the three-step test plus provision, public access and use of intellectual property is no longer just an abstract or nebulous policy recommendation to guide legislators, regulators and courts in interpreting or implementing the law, but it has become a substantive legal requirement that must be employed to evaluate and judge the legitimacy or propriety of various forms of access to and uses of intellectual property.

The three-step test plus provision is meant to promote greater creativity and innovation for both authors and creators and society as

whole. The WIPO Standing Committee on the Law of Patents explains the rationale for the additional wording: “the scope of the enforceable exclusive rights is carefully designed under national patent laws in order to strike the right balance between the legitimate interests of the right holders and the legitimate interests of third parties”.²⁰³ Affirming the desirability of preserving the intellectual property balance, the Committee states:

the exclusive rights conferred by a patent and the exceptions and limitations to such rights are two sides of the same coin seeking to balance the legitimate interests of the patent owner and the legitimate interests of third parties with a view to promote innovation, disseminate technical knowledge and encourage transfer of technology.²⁰⁴

With the inordinate focus on broadening and strengthening the exclusive rights granted to creators and inventors in past decades, the public interest goals and social objectives of intellectual property laws have been neglected. The three-step test plus provision reaffirms and reasserts that intellectual property has “the ultimate goal of promoting innovation and enhancing public welfare”.²⁰⁵ The grant of intellectual property rights is therefore meant “to promote innovation and to improve the social benefits resulting from that innovation”.²⁰⁶ As a consequence, the “underlying consideration is that the public interest justifies, under certain circumstances, denying the enforcement of the exclusive rights granted to patentees” as well as other creators for the benefit of the public.²⁰⁷

While the three-step test plus is already contained in the TRIPS

²⁰³ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 19; see also Lawrence Lessig, Code: version 2.0 183.

²⁰⁴ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 25.

²⁰⁵ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 2, 3 and 19.

²⁰⁶ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 2.

²⁰⁷ WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” 19; see also Lawrence Lessig, Code: version 2.0 183.

Agreement, it is such a monumental provision that it should be incorporated as well into other international, regional and national laws and applied to other forms of intellectual property and not just patents and industrial designs. Since the principle of the intellectual property balance applies to all intellectual property rights and the three-step test plus provision superbly encapsulates and upholds this balance, it seems logical to apply the three-step test plus as well to copyright and other forms of intellectual property. This would require either updating the wording of the three-step test in these laws to include the phrase “taking account of the legitimate interests of third parties”, or, more simply, national courts or adjudicatory bodies can read the phrase into the law or render judgment that it is applicable in their jurisdictions. While this is a seemingly minor amendment to the law, it has far-reaching consequences that can benefit hackers and society as a whole. Patents are particularly problematic for makers because the grant of rights to patent holders is so extensive that it effectively bars them from publicly and openly developing and distributing a project (e.g., a 3D printer) that involves a protected invention (e.g., an essential technology for 3D printing) even though the project is non-commercial and open source. With a three-step test plus provision in place, a judge or court would have to take into account as well the legitimate interests of makers, the hacker community and those of the general public in arriving at the decision. This is much better than the original wording of the three-step test where only the interests of the owners and creators are considered. Given that the great majority of hacker projects and activities (especially those of makers) are undertaken for personal and non-commercial purposes and with a view to producing new technologies or innovative uses for the benefit of their communities and the wider society, then such acts of hacking will most likely be deemed permissible or excepted under the proposed three-step test plus provision.

6.3.3 ANTI-CIRCUMVENTION AND CONTRACT LAWS

6.3.3.1 More limitations and exceptions to anti-circumvention

Anti-circumvention rules as currently worded and applied seriously hinder the ability of makers, hacktivists and ordinary users from accessing information and creatively using their technologies. Since it is highly unlikely and it would not be reasonable to expect or demand the complete abolition of anti-circumvention rules given the well-entrenched regime of international, regional and national laws that support them, the sensible option then is to work within the legal framework and introduce and develop more limitations and exceptions in the law. Many countries in Europe, including the Netherlands, have not formally adopted specific limitations and exceptions to the anti-circumvention prohibitions despite an express provision in the Copyright Directive allowing them to do.²⁰⁸ Therefore, the first step in improving anti-circumvention laws would be for states to explicitly provide in their national laws specific limitations and exceptions to the prohibitions against circumvention such as for teaching and scientific research and for private and non-commercial use as stated in the Copyright Directive.²⁰⁹ Furthermore, European countries would do well to further clarify and enhance the list of limitations and exceptions to anti-circumvention that are contained in the Copyright Directive particularly in relation to temporary acts of reproduction, repair, and even the three-step test (or fair use if applicable). Countries may also draw inspiration from the United States whose anti-circumvention legislation lays down specific limitations and exceptions for activities such as encryption research, security testing, and protecting personally

²⁰⁸ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, art 6(4); European Commission, "Report on the application of the Directive 2001/29/EC" SEC(2007) 1556, 9; see also Urs Gasser and Michael Girsberger, "Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States" 22 and 30.

²⁰⁹ Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, arts 6(4).

²¹⁰ 17 U.S. Code section 1201, arts (g), (i) and (j); see also Derek Bambauer and Oliver Day, "The Hacker's Aegis" 31.

identifying information.²¹⁰ Another possible model for European law is the triennial review procedure adopted in the United States where the US Librarian of Congress reviews the anti-circumvention rules every three years with the aim of establishing new limitations and exceptions based on current technologies and practices.²¹¹ It should be noted that the Copyright Directive does state that the “legal protection” of technological protection measures “should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography”.²¹² These exemptions would prove quite valuable to makers and hackers since many of their hacking projects and activities concern information security and privacy protection.

In light of the values and goals sought to be protected and promoted by copyright laws vis-à-vis anti-circumvention laws, it can justifiably be argued that all activities that fall within any of the statutory limitations and exceptions to copyright and related rights should be automatically or presumptively *prima facie* exempted from the application of anti-circumvention rules since such acts are legitimate or permitted under the law.²¹³ While this interpretation is implied in the legislative context and purposes of anti-circumvention laws, so as to avoid any doubt and promote legal certainty, there should be an explicit legal provision (or alternatively, a judicial or policy confirmation) that anti-circumvention rules do not or should not apply or interfere with existing and future limitations and exceptions to copyright and related rights. US anti-circumvention rules contain such a provision, which incontrovertibly states: “Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement,

²¹¹ 17 U.S. Code section 1201, arts (a)(1)(B)-(D); see also Pamela Samuelson, “Freedom to Tinker” 19; see also Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 32.

²¹² Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, recital 48.

²¹³ See Daniel Gervais, “A Principled Approach to Copyright Exceptions and Limitations” 22.

²¹⁴ 17 U.S. Code section 1201, art (c)(1) (emphasis added).

including fair use, under this title”.²¹⁴ A similar statutory provision or policy statement can be adopted in the laws of countries like the Netherlands where no such an express doctrine exists.

6.3.3.2 Necessary nexus between circumvention and copyright infringement

Aside from the need to have additional and more explicit limitations and exceptions to anti-circumvention rules, many of the problems and issues hounding technological protection measures can be remedied by reiterating, as a matter of public policy, that these rules should only apply in cases where the act or technology of circumvention is reasonably connected to actual or potential copyright infringement. This proposal seems self-evident but, as described in Section 4.4.2.2, anti-circumvention laws have been applied or sought to be enforced in situations that have absolutely nothing to do with copyright piracy. This goes against the intent of both copyright laws and anti-circumvention rules. As the European Commission clearly states:

According to the Directive, the protection of TPM [technological protection measures] complements the protection of copyright. The Directive only requires Member States to protect TPM in respect of works or any subject-matter covered by ‘copyright or any right related to copyright as provided by the law or the sui generis right in databases’. TPM applied to protect other subject matter or works in the public domain are thus not protected under the Directive.²¹⁵

The European Commission further clarifies that, “Article 6(3) [of the Copyright Directive] requires that TPM are applied to restrict acts which are not authorised by the rightholders of the protected subject matter.... This implies that Article 6(3) only protects technological measures that restrict acts which come within the scope of the exclusive rights”.²¹⁶ The Commission’s interpretation is based on the text of

²¹⁵ European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 7.

²¹⁶ European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 7.

the WIPO Copyright Treaty, which states that the protected technological measures are those used “in connection with the exercise of their [authors’] rights under this Treaty or the Berne Convention” (i.e., copyright and related rights).²¹⁷ Article 12 of the WIPO Copyright Treaty also provides that circumvention of rights management information is unlawful if “it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention”.²¹⁸ Anti-circumvention rules are “therefore aimed at preventing an act which would amount to an infringement of copyright”.²¹⁹ For this reason, absent this indispensable connection between circumvention and copyright infringement,²²⁰ the anti-circumvention rules should not apply. This was the conclusion as well in the landmark US case of *Chamberlain Group v Skylink Technologies* where the Court of Appeals held that:

The DMCA [Digital Millennium Copyright Act] does not create a new property right for copyright owners. Nor, for that matter, does it divest the public of the property rights that the Copyright Act has long granted to the public. The anti-circumvention and antitrafficking provisions of the DMCA create new grounds of liability.... A copyright owner seeking to impose liability on an accused trafficker must demonstrate that the trafficker’s device enables either copyright infringement or a prohibited circumvention.... This connection is critical to sustaining a cause of action under the DMCA.”²²¹

Thus, lacking “the critical nexus between access and protection” no claim can be filed and no liability should attach under anti-circumvention laws.²²² According to the Court, “the broad policy implications of considering ‘access’ in a vacuum devoid of ‘protection’ are both absurd and disastrous”.²²³ The Court explained that,

²¹⁷ WIPO Copyright Treaty, art 11.

²¹⁸ WIPO Copyright Treaty, art 12.

²¹⁹ European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 8.

²²⁰ See European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556, 7.

²²¹ *Chamberlain Group v Skylink Technologies* 381 F. 3d 1178 (2004), 1204 (emphasis added).

²²² *Chamberlain Group v Skylink Technologies* 381 F. 3d 1178 (2004), 1204 (emphasis added); see also Pamela Samuelson, “Freedom to Tinker” 19.

²²³ *Chamberlain Group v Skylink Technologies* 381 F. 3d 1178 (2004), 1200-1201.

“This distinction between property and liability is critical. Whereas copyrights, like patents, are property, liability protection from unauthorized circumvention merely creates a new cause of action under which a defendant may be liable”.²²⁴ Examining the legislative histories of both the WIPO Copyright Treaty and the US Digital Millennium Copyright Act (DMCA), the Court ruled, “circumvention is not a new form of infringement but rather a new violation prohibiting actions or products that facilitate infringement”.²²⁵ The Court ultimately concluded that DMCA “prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners”.²²⁶

In light of the crucial requirement that there must be a nexus between circumvention and copyright infringement for anti-circumvention rules to apply, most makers and hacktivists would not run afoul of the law since their circumvention activities do not usually involve infringing copyrighted materials and they largely fall within existing limitations and exceptions or widely recognized normal or customary uses of intellectual property such as reverse engineering, decompilation for purposes of interoperability, scientific research, personal and non-commercial use, and time, place and format shifting of content.²²⁷ Following this recommended interpretation of anti-circumvention rules, which can be judicially confirmed by the relevant court, hackers should be able to lawfully hack technological protection measures and have reasonably free and open access to the information and technologies that they legitimately own, possess, create or remake.

²²⁴ Chamberlain Group v Skylink Technologies 381 F. 3d 1178 (2004), 1192-1193.

²²⁵ Chamberlain Group v Skylink Technologies 381 F. 3d 1178 (2004), 1197.

²²⁶ Chamberlain Group v Skylink Technologies 381 F. 3d 1178 (2004), 1202 (emphasis added); see also Pamela Samuelson, “Freedom to Tinker” 19 and 21; but see MDY Industries v Blizzard Entertainment, 629 F. 3d 928 (2010); see also Pamela Samuelson, “Freedom to Tinker” 19 (the MDY case “rejecting the nexus to infringement requirement set forth in Chamberlain”); see also Universal City Studios v Reimerdes 111 F.Supp.2d 294 (2000), Universal City Studios v Corley, 273 F.3d 429 (2001).

²²⁷ See Pamela Samuelson, “Freedom to Tinker” 19 and 23; see Lawrence Lessig, Code: version 2.0 191.

6.3.3.3 No contractual waivers of limitations and exceptions

As shown in the preceding chapters, freedom of contract when applied in combination with intellectual property laws can be a double-edged sword. Contracts can impair the rights of users through restrictive terms of service and licensing agreements, but they can also allow members of the public (including hackers) to freely use and openly access information and technologies through the use of copyleft and other free and open source licenses. In any event, contract law can still be improved in order to advance rather than impede cultural change and technical innovation. For one, the rules that prohibit any contractual waiver, diminution or bargaining away of the rights to reverse engineer, decompile, correct errors, and make back-up copies of computer programs should be applied as well to other fundamental limitations and exceptions to intellectual property rights.²²⁸ According to Samuelson, “[c]ourts and legislatures should be willing to affirm the ownership interests of purchasers of digital content that should not be overridden by mass-market license restrictions”.²²⁹ Since undertaking legislative reform will take much time and effort, it would be quicker and simpler for the relevant national courts to render judgment or set a precedent that the prohibition against contractual waivers should likewise cover other limitations and exceptions such as private and non-commercial copying and use, scientific research and teaching, repair, and the three-step test or fair use. Limitations and exceptions are extremely valuable to hackers because these serve as the legal bases for them to explore and study, creatively hack and satisfy their curiosity about technologies or creative works.

Extending the bar against contractual waivers to include other limitations and exceptions to intellectual property rights is imperative because, not only are they few and far between, but they are also the primary mechanisms by which the all-important intellectual property

²²⁸ See Directive 2009/24/EC on the legal protection of computer programs, arts 5 and 6 and recital 13.

²²⁹ Pamela Samuelson, “Freedom to Tinker” 23.

balance is preserved. Surely, the legal principles and public interest rationales that underlie the intellectual property regime, which aim to maintain a careful balance between the rights of creators vis-à-vis the rights of the public, should not be defeated or nullified through the mere expedient of resorting to contractual stipulations to the contrary. Laws and matters of public policy should not be so easily set aside. Members of the hacker community, most especially makers, would benefit from a legal prohibition against contractual waivers of limitations and exceptions as this would ensure that those permitted or excepted uses granted to them under the law (e.g., private and non-commercial use) would be preserved. In this way, what hackers and users can or cannot do with a creative work or invention is set out and determined by laws and jurisprudence and not the one-sided contractual terms imposed by intellectual property owners.

6.3.4 RIGHTS OF USERS

Another way to improve the laws on hacking is for public authorities to recognize and respect the rights of users. This requires making the crucial distinction between commercial and non-commercial²³⁰ and malicious versus benign²³¹ users and uses of information and technologies. Existing laws and policies generally tend to lump together ordinary users with commercial infringers in relation to intellectual property and contracts, and to conflate hackers with malicious attackers in matters concerning computer crime and anti-circumvention.²³² The problem with the overly broad, restrictive and punitive application of these laws is that, while their purported aims are to arrest, punish or deter acts that are threatening, harmful or cause damage, they inevitably end up interfering with or penalizing normal, de mini-

²³⁰ See Barton Beebe, "An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005" 597-603; see Creative Commons, "Defining 'Noncommercial'".

²³¹ Richard Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws" 104; see also Oliver Wendell Holmes, Jr., "Privilege, Malice, and Intent".

²³² Pamela Samuleson, "Freedom to Tinker" 2.

mis or even innovative activities and practices of ordinary users and hackers. More can be done to make technology laws and policies more precise and nuanced in their application and impact. In the context of computer crime laws, introducing the element of criminal intent can help public authorities more fairly and effectively distinguish between permissible acts of hacking as opposed to unlawful cyber attacks. With respect to intellectual property laws, recognizing the difference between non-commercial uses versus those that are commercially infringing or damaging can be done by examining the specific user and uses of a protected work in a particular case, and interpreting or applying an existing limitation and exception or the proposed three-step test plus provision strictly against commercial infringers but favorably when it comes to ordinary users.²³³ Differentiating between commercial and non-commercial uses is admittedly not an easy or straightforward task but the distinction can and has to be made otherwise ordinary users (including hackers) may be penalized for undertaking common, benign or creative activities. This is not say that ordinary users are free from liability for copyright infringement (e.g., in the case of peer-to-peer file sharing). However, the law and the courts should distinguish between ordinary users and commercial infringers and only impose reasonable restrictions on and appropriate penalties for the respective groups.²³⁴

In order to properly distinguish creative and common users and uses from those that are malicious and infringing, it is essential for the law and public authorities to affirm or recognize people's right to hack the information and technologies that they lawfully produce, own or possess. As discussed throughout this book, this right to hack includes the ability to explore, break, learn, create, share and secure

²³³ Debora Halbert, "Mass Culture and the Culture of the Masses: A Manifesto for User-Generated Rights" 958; see also Urs Gasser and Silke Ernst, "A Quick Look at Copyright and User Creativity in the Digital Age" 10.

²³⁴ See Pamela Samuleson, "Freedom to Tinker" 23.

technologies and intellectual creations. It is about the “freedom to understand, discuss, repair, and modify the technological devices you own” and creatively use the content or information that one has.²³⁵ As Samuelson explains,

[p]eople tinker with technologies and other human-made artifacts for a variety of reasons: to have fun, to be playful, to learn how things work, to discern their flaws or vulnerabilities, to build their skills, to become more actualized, to tailor the artifacts to serve one’s specific needs or functions, to repair or make improvements to the artifacts, to adapt them to new purposes, and occasionally, to be destructive.²³⁶

The freedom to hack or tinker is the crux or cornerstone that underpins many user rights in the information age. The significance of hacking and tinkering is that they enable “freedom of thought, study, inquiry, self-expression, diffusion of knowledge, and building a community of highly skilled tinkerers. In addition, freedom to tinker fosters privacy, autonomy, human flourishing, and skills building interests”.²³⁷ Whether one calls it the right to hack or freedom to tinker, according to Samuelson, it necessarily involves or requires:

first, an intellectual freedom to imagine what one might do with existing artifacts to learn more about them; second, an intellectual privacy and autonomy interest in investigating and exploring those artifacts in which one has a property or other legitimate interest, especially when the investigation is done in one’s own premises; third, a right to build one’s skills by testing, analyzing, and interacting with existing artifacts; fourth, a liberty interest to become more actualized as a person through tinkering; fifth, a right to distill what one has learned from tinkering and disseminate the results of one’s research to others; sixth, a right to repair that which is broken and make other uses of artifacts as long as one is not harming the interests of others; seventh, a right to innovate based on what one has learned through tinkering; and eighth, a right to share innovations that

²³⁵ Pamela Samuleson, “Freedom to Tinker” 2 (citing Edward Felten).

²³⁶ Pamela Samuleson, “Freedom to Tinker” 1-2.

²³⁷ Pamela Samuleson, “Freedom to Tinker” 21.

result from tinkering with others if one chooses to do so and build a community around the innovation.²³⁸

These are basically the same digital rights and technological freedoms that are expressed and demanded by makers, hacktivists and other hackers in their manifestos (see Section 3.3.2). For example, they have articulated and advocated for the following user rights and freedoms: to create,²³⁹ to repair,²⁴⁰ to make, share, learn about and change our own devices,²⁴¹ to fix and improve,²⁴² to “open and repair our things without voiding the warranty”,²⁴³ “to devices that can be opened”, “to repair things in the privacy of our own homes”,²⁴⁵ “to hardware that doesn’t require proprietary tools to repair”,²⁴⁶ “to run, copy, distribute, study, change and improve... software”,²⁴⁷ to “free and equal access to all publicly-produced information”,²⁴⁸ and to free access to computers and information.²⁴⁹ Whether for hackers or ordinary users, it is crucial to preserve and promote these freedoms associated with hacking and tinkering because they “generally ‘promote the progress of science and useful arts,’ as well as other fundamental values”.²⁵⁰

In sum, while formal legal reform through legislative amendments or judicial rulings are ultimately needed to provide legal certainty and clarity and to fully carry out the preceding legal recommendations, based on the successful outcomes of the responsible disclosure rules and open data hackathons in the Netherlands, it appears that a change in technology policy, greater participation of and collaborations with hackers and the public, and other soft law approaches offer

²³⁸ Pamela Samuleson, “Freedom to Tinker” 2.

²³⁹ Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age* 139-141.

²⁴⁰ Platform21, “Repair Manifesto” <www.platform21.nl/download/4375> accessed 28 November 2012.

²⁴¹ Mark Hatch, *The Maker Movement Manifesto* 1-2.

²⁴² Sugru, “The Fixer’s Manifesto” <<https://raw.githubusercontent.com/sugru/manifesto/master/manifesto.pdf>> accessed 20 April 2016.

²⁴³ iFixit, “Self-Repair Manifesto” <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014.

²⁴⁴ iFixit, “Self-Repair Manifesto” <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014.

²⁴⁵ iFixit, “Self-Repair Manifesto” <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014.

²⁴⁶ iFixit, “Self-Repair Manifesto” <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014.

²⁴⁷ “The Free Software Definition” <www.gnu.org/philosophy/free-sw.html> accessed 2 July 2013.

²⁴⁸ Elen Moglen, “The dotCommunist Manifesto” <http://emoglen.law.columbia.edu/my_pubs/dcm.html> 23 February 2014.

²⁴⁹ Steven Levy, *Hackers* 28-34.

²⁵⁰ Pamela Samuleson, “Freedom to Tinker”

more immediate and practical solutions to improving the laws on hacking.

6.4 Hacking can be change for good

The legal and normative recommendations proposed above are fairly straightforward and do not require unreasonable costs and efforts to implement. The suggested improvements to regulatory approaches and policies concerning hacking are based on an extensive and empirically grounded analysis of both the socio-technical practices of hackers and the laws that affect them. However, in spite of the strong empirical and legal bases to support these proposals, I am well aware that undertaking such reforms will still most likely face strong objections from certain sectors (e.g., commercial companies, law enforcement agencies and government departments) and will be politically contentious.²⁵¹ This is expected given the lack of progress in reforming computer crime laws even after the much-publicized suicide of hacktivist Aaron Swartz, who at the time of his death was being criminally prosecuted and faced years of imprisonment for trying to make publications in an academic database accessible to a wider public.²⁵² There were attempts in the United States to amend the law, including one called “Aaron’s Law”.²⁵³ According to the sponsors of the bill, “Aaron’s Law is... about refocusing the law away from common computer and Internet activity and toward damaging hacks.... distinguish the difference between common online activities and harmful attacks²⁵⁴ Aaron’s Law sought “to bring balance back to” the US Computer Fraud and Abuse Act by including the qualification of infringing a security measure as a requirement for illegal access.²⁵⁵ However,

²⁵¹ See Derek Bambauer and Oliver Day, “The Hacker’s Aegis” 42 and 43.

²⁵² Glenn Greenwald, “The inspiring heroism of Aaron Swartz”; Lothar Determann, “Internet Freedom and Computer Abuse” 429.

²⁵³ Sarah Constant, “Computer Fraud and Abuse Act: A Prosecutor’s Dream and a Hacker’s Worst Nightmare - The Case Against Aaron Swartz and the Need To Reform the CFAA” 244-245; see also Mark Murfin, “Aaron’s Law: Bringing Sensibility to the Computer Fraud and Abuse Act” 479.

²⁵⁴ Zoe Lofgren and Ron Wyden, “Introducing Aaron’s Law”.

²⁵⁵ Zoe Lofgren and Ron Wyden, “Introducing Aaron’s Law”.

these efforts to improve computer crime laws “appear to be foundering” and “Aaron’s Law would not be passing”.²⁵⁶ According to Maker H, “The Aaron Swartz movement never got any real traction on Capitol Hill as far as my understanding goes”.²⁵⁷ Without a doubt, the revelations of Edward Snowden played a part in hampering the passage of Aaron’s Law and other similar reforms. According to Fakhoury, “Before Edward Snowden showed up, 2013 was shaping up as a year of reckoning for the much criticized federal anti-hacking statute, the Computer Fraud and Abuse Act”.²⁵⁸ The current attitude of public authorities to amending computer crime laws can be described in this way:

But unfortunately, not much has changed; if anything, the growing recognition of the powerful capabilities of modern computing and networking has resulted in a ‘cyber panic’ in legislatures and prosecutor offices across the country. Instead of reexamination, we’ve seen aggressive charges and excessive punishment.²⁵⁹

So, the reverse is happening – there have been moves to further ratchet up the law. This is, of course, in line with the historic tendency of computer crime laws to become all the more restrictive and punitive.²⁶⁰ According to the Electronic Frontier Foundation, “As if the law’s current magnitude of punishment isn’t overwhelming enough, Congress has been thinking about beefing up” the US Computer Fraud and Abuse Act.²⁶¹ Rather than making the law less restrictive in order to accommodate benign or productive activities like hacking, because of the Snowden revelations and many high profile security breaches, “many want to see [the Computer Fraud and Abuse Act] punishments made more severe”.²⁶² Even the amended Cybercrime

²⁵⁶ Tom Brewster, “US cybercrime law being used to target security researchers”.

²⁵⁷ Interview with Maker H.

²⁵⁸ Hanni Fakhoury, “The U.S. Crackdown on Hackers Is Our New War on Drugs”.

²⁵⁹ Hanni Fakhoury, “The U.S. Crackdown on Hackers Is Our New War on Drugs”.

²⁶⁰ Reid Skibell, “Cybercrimes & Misdemeanors” 911.

²⁶¹ Electronic Frontier Foundation, “Let’s Fix Draconian Computer Crime Law”; see also Sarah Constant, “Computer Fraud and Abuse Act: A Prosecutor’s Dream and a Hacker’s Worst Nightmare - The Case Against Aaron Swartz and the Need To Reform the CFAA” 247; see also Mark Murfin, “Aaron’s Law: Bringing Sensibility to the Computer Fraud and Abuse Act”.

²⁶² Tom Brewster, “US cybercrime law being used to target security researchers”.

Directive considers it “appropriate to provide for more severe penalties”.²⁶³ While the imposition of harsher penalties may be appropriate for malicious attackers and cybercriminals, unless a clear distinction is made in the law between destructive cyber attacks and the innocuous activities of hackers, hacking will remain over-criminalized.

It is evident that for the improvements recommended in this book to come to fruition they must be accompanied by cultural change most especially on the part of the law and public authorities. Without this metanoia, no genuine or effective legal change can be expected. Nevertheless, even though reforms may appear distant or slow to come, hackers as well as ordinary citizens and users can still aim to reshape the law through their everyday practices and the very technologies that they make and use. While entrenched government culture may impede the improvement of hacking-related laws, socio-cultural change can serve as a starting point or impetus for much needed legal reform. Recall that, in relation to intellectual property laws, FOSS developers were able to fundamentally remake how software is developed, licensed and used, not by political lobbying, but through their individual choices and group actions and the novel use of intellectual property licenses to ensure that computer programs are free and open for everyone to use.

In a similar vein, the collaborative and bottom-up approach of the responsible disclosure rules has helped make the enforcement of computer crime laws more nuanced and can ultimately result in better information security for private and public individuals and entities. Cultural change in the form of developing techno-social practices like bug bounty programs can likewise impact computer crime laws (see Section 6.2.1.1). What is noteworthy about bug bounty programs is

²⁶³ Council Directive 2013/40/EU on attacks against information systems, recital 13.

²⁶⁴ See Cassandra Kirsch, “The Grey Hat Hacker” 385 and 398.

²⁶⁵ See Cassandra Kirsch, “The Grey Hat Hacker” 397.

how hackers and commercial companies are able to develop legitimate and common practices and rules that are mutually beneficial to them and actually result in improved computer security,²⁶⁴ despite or regardless of computer crime laws. Bug bounty programs can attribute their success to companies being more open to working with hackers and treating them as equal partners or co-participants in information security.²⁶⁵

In this way, even though reforms to hacking-related laws may not be immediately forthcoming, hackers and other actors in the networked information society (including ordinary users and citizens) will continue to carry out and develop their own customs and conduct concerning access to and use of information and technology. As long as these practices and technologies are not incompatible with fundamental rights and democratic values, once they become established and internalized as legitimate and common activities by the relevant community and society as a whole, it would be reasonable for the law to recognize and build on the socio-technical rules that are already in place. This is so because, particularly in relation to technological and cultural innovation, laws should ultimately reflect as well as promote existing and changing norms and values. As with hacking, this can be change for good.

Epilogue: The value and future of socio-techno-legal studies

7.1 For law and policymaking

As this book has demonstrated, makers and hacktivists are part of a longstanding, well-developed and vibrant hacker culture that has its own distinguishing technologies, practices, norms and values. There are different types of hackers and most of them, including the makers and hacktivists who are the subject of this book, are far from being the malevolent outlaws depicted in popular and mass media who are hell-bent on damaging computers and data for malicious reasons. While they are admittedly neither angels nor saints and they would not consider themselves law-abiding, the hackers I met care for fundamental rights and freedoms and respect democratic values. They may be extremely enthusiastic about and can do quite amazing feats with technology, but they are also social actors who have their own deeply held beliefs and rules of behaviors. Hackers highly prize technical creativity and innovation and mastery over technology, however they are also very much aware of the social impact of technology and their social responsibility when using or designing it. Their norms and values are also intimately connected with liberal democratic principles and goals. Makers and hacktivists cherish individual autonomy and liberty but they also use their personal freedoms for the benefit of the hacker community and the wider public whether through the creation of open source 3D printers that anyone can freely build and use or

through engagement in campaigns to improve the security of private and public information systems. They wholeheartedly strive for openness, transparency and freedom of access to information and technology, yet they also insist on protecting privacy and security, especially for the weak and marginalized in society.¹ They engage in hacking projects and activities for both personal motives and social ends. Aside from breaking, hacking for them is equally about exploring technologies or technical systems, learning how they work, creating something new or surprising, sharing their creations with others, and securing information and technology for the benefit of themselves and society.

Having such a deep-seated worldview and strongly held rules and standards of the acceptable and desirable, it is no wonder then that hackers have such a conflicted history and relationship with law and public authorities. Makers and hacktivists dislike centralized authorities and hierarchies. On the whole, hackers would rather ignore and have nothing to do with the law or deal with legal issues. However, when it becomes impossible to avoid the law or if engaging with the law is a means to a social end, hackers will endeavor to change the law mainly through technical means and devices, but they may also do so by using, adapting or working within the legal system. In the same way that hacking is about non-conformity with the normal rules and expected uses of technology, hackers can challenge legal rules and government actors and strive to subvert their authority when necessary.

Pursuant to this book's findings, it is important for law and policymakers to first understand and take account of the robust and deeply rooted hacker culture before they adopt or try to implement laws and policies that affect hackers or adversely impact the free and open access to and use of information and technology. Otherwise,

¹ See Chapters 3 and 5; see Julian Assange and others, *Cyberpunks* (Audible 2013) (many hackers subscribe to the creed of "privacy for the weak, transparency for the powerful"); see Chaos Computer Club, "hackerethics" <<http://www.ccc.de/hackerethics>> accessed 17 July 2013.

these laws can have negative effects and unintended consequences not just on hacking but also on how people in general develop and use technology. Quite a number of technology laws and policies concerning hacking like anti-circumvention laws have not succeeded in achieving their stated goals or have produced unforeseen or problematic outcomes because they seemingly perceive hackers as mere regulatory targets or “pathetic dots”² who have no choice but to conform to laws that have been imposed on them from the top-down (see Section 4.4.2). But this view is not borne out by the research. As seen in Chapter 5, especially in the campaign against the use of electronic voting machines (see Section 5.2.2.2), makers and hacktivists are “active subjects”³ who resist, contest, negotiate and change laws. This is especially true since, in a highly technological and connected world, hackers and other technical and epistemic groups are possessors and purveyors of much agency and power that can be utilized for technical, social and even legal purposes.

It therefore behooves public authorities to recognize and consider hacker practices, norms and values when developing technology laws and policies that impact hacking. This means restraining the impulse to immediately or sweepingly regulate hacking projects and activities merely because they are new or disruptive or there is fear and moral panic among authorities and the public who do not yet fully understand them. As seen in the case of computer crime laws, without a proper understanding of hacker culture, technology laws and policies can be overly broad that they end up prohibiting creative or benign forms of hacking (see Section 4.2.3). Public authorities should at least be knowledgeable about the culture and technologies of the persons, activities or fields that they desire to regulate. This can be achieved, for

² See Lawrence Lessig, Code version 2.0 122-123.

³ See John Morison, “Modernising Government and the E-Government Revolution” 158 and 162-163; see Michael Dizon, “Free and Open Source Software Communities, Democracy and ICT Law and Policy” 134.

⁴ Lawrence Lessig, Code version 2.0 123 and 130.

example, by means of legislative investigations, public hearings and consultations with the subject group or community, requests for comments or responses to proposed regulation from the relevant stakeholders, reference to existing academic literature, or funding further scientific research on the matter. While many law and policymakers already undertake these processes, there must be a genuine attempt to understand the culture and practices of the subject persons or fields and it should actually influence or help determine the legal and policy outcomes and not be a mere formality. Based on their improved understanding of the subject social group or community, public authorities can then decide whether to regulate at all or which appropriate modalities of regulation to adopt (i.e., law, social norms, technology, the market, or a combination or hybrid of these) that are best suited or will optimally produce the desired regulatory goals, but bearing in mind the specific norms, values and social contexts of the regulatory subject. Furthermore, even after the regulatory approach is chosen and implemented, it is crucial to have a regular review and evaluation of the regulation in order to guard against unforeseen or unexpected effects and to continually improve the law based on the actual results or outcomes that it has engendered.⁵ As evinced in Chapters 4, 5 and 6, such socio-legal analyses and empirical assessments are necessary to improve computer crime, intellectual property, contract and anti-circumvention laws, as well as laws in general.

Law and policymakers should resist applying as default the “command and control” approach to regulation, which entails selecting a social field or activity that they wish to control and impose order from above, because it may be incompatible or come into conflict with existing cultures and legitimate practices.⁶ Laws are not the only origin

⁵ See Andrew Murray, *The Regulation of Cyberspace* 248 (use of feedback loops)

⁶ See Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation* 80-81 (on traditional “command and control” regulation); see also Roger Brownsword, “Code, control and choice” 1; see John Griffiths, “What Is Legal Pluralism?” 38 (for a critique of “legal centralism”); see also Michael Dizon, “Law and Networks” 18.

or source of norms and other rules of social behavior, and it would be wise for public authorities to take these into consideration when deciding what legal action or policy decision they should or should not take.⁷ Regulating hackers or indeed any other social group or community is not that straightforward since the relevant social field or activity is far from lawless and it is constituted and thickly permeated by its own standards and expectations of the appropriate and desirable. Public authorities should avoid imagining socio-technical fields as an untamed frontier or no man's land that have no rules or restrictions and which either could or could not be settled and put into order through government intervention.⁸ Contrary to this simplistic viewpoint, there is no normative vacuum in these techno-social fields since in reality individuals and groups reside and inhabit these spaces and they have their own internal rules of governance or control. In fact, as seen in the case of hackers, the norms and values of social groups and subcultures can extend or emanate out of their social fields either organically or sometimes even forcefully from the bottom-up and impact the general public (see Sections 5.2.2.2 and 5.2.2.3 on the hacking of the electronic voting computers and Leaktober).⁹ Non-states actors like hackers can and do play a vital role in determining what is normative in society. Thus, as evident in the cases of the responsible disclosure rules and open data hackathons (see Sections 6.2.1 and 6.2.2), it would be wiser and more productive for public authorities to treat makers and hacktivists not as regulatory threats and targets but as genuine co-participants or potential collaborators in the development of technology laws and policies, especially those that concern hacking. Despite their general distrust or aversion to centralized authorities,

⁷ See John Griffiths, "What is Legal Pluralism?"; Boaventura de Sousa Santos "Toward a Postmodern Conception of Law"; Sally Falk Moore, "Law and Social Change"; Franz von Benda-Beckmann, "Who's Afraid of Legal Pluralism?"; Brian Tamanaha, "Understanding Legal Pluralism"; Anne Griffith, "Legal Pluralism"; Jack Gibbs, "The Sociology of Law and Normative Phenomena".

⁸ See for example David Johnson and David Post, "Law and Borders - The Rise of Law in Cyberspace"; see Carolyn Penfold, "Nazis, Porn and Politics: Asserting Control Over Internet Content"; see Llewellyn Joseph Gibbons, "No Regulation, Government Regulation, or Self-regulation"; see Jack Goldsmith, "Regulation of the Internet: Three Persistent Fallacies".

⁹ See Chapter 5.

hackers too should be more open and willing to assist and work with public authorities and share their knowledge, skills and perspectives to improve or make better laws. Sharing their technical expertise and know-how is particularly relevant given that hackers' primary criticism or complaint about public authorities is the latter's lack of in-depth technical knowledge and understanding of the technologies and practices that are the objects of regulation.¹⁰ As presented in Section 6.2, constructive collaborations between hackers and public authorities are underway in the Netherlands with the active involvement of makers and hacktivists with the responsible disclosure rules and open data hackathons. These collaborative efforts are steps in the right direction and should be emulated by other countries.

7.2 For law and technology research

In the same way that law and policymakers can profit from a more thorough understanding of the social fields or activities that they seek to regulate, law and technology research can also derive much benefit from the socio-techno-legal approach applied in this book. Law and technology scholars are admittedly ahead of public authorities in terms of their appreciation of the importance of knowing more about how a specific technology works and its ramifications on existing or proposed regulation. In essence, most if not all technology law scholarship is about describing and analyzing the interactions between the technical and the legal. In fact, technology law scholars have been so successful in their technology-centered approach that they have been pooh-poohed for being so enamored with technology and overly focused on the technical nitty-gritty.¹¹ However, since the early cyberlaw literature, the depth and breadth of internet and information technology law research has grown tremendously and its pos-

¹⁰ Interviews.

¹¹ See Frank Easterbrook, "Cyberspace and the Law of the Horse".

itive contributions to legal theory, policy and practice have proved the criticism unfounded.¹² Information technology and networks mediate and shape so much of people's lives that ignoring them and their legal implications and social effects would be unwise.

While technology law scholars have the technical and legal aspects down to pat, they as well as researchers from other areas or disciplines could gain much in terms of improving the coherence, credibility and significance of their research by equally focusing on the often neglected social dimensions of a new or disruptive technology or technical activity.¹³ Technology, like law, is semi-socially constructed and constructing.¹⁴ Much literature in socio-legal studies is about the social construction and embeddedness of law and the stark difference between black letter law (law in books) and the law as experienced in everyday life (law in action).¹⁵ Similarly, most STS research is devoted to explicating the co-production of technology and society.¹⁶ This means that, to further or fully comprehend and evaluate the legal and social impact of a technical practice such as hacking or a technology like 3D printing, it is indispensable for technology law research to examine the social practices, beliefs and contexts of the persons or groups involved, including the norms and values embedded and enacted in their technologies or technical activities.¹⁷ For their part, tech-

¹² See Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach"; see Lawrence Lessig, *Code and Other Laws of Cyberspace*; see Christopher Marsden (ed), *Regulating the Global Information Society*; see Jessica Litman, *Digital Copyright*; see Lawrence Lessig, *Free Culture*; see Peter Drahos and John Braithwaite, *Information Feudalism*; see James Boyle, *The Public Domain*; see Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*; see Yochai Benkler, *The Wealth of Networks*; see Jonathan Zittrain, *The Future of the Internet*; see Andrew Murray, *The Regulation of Cyberspace*; see Tim Wu, *The Master Switch*; see Andrew Murray, "Looking Back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important".

¹³ See Alan Bryman, *Social Research Methods* 393 and 396.

¹⁴ See Trevor Pinch and Wiebe Bijker, "The Social Construction of Facts and Artefacts"; see Sheila Jasanoff, "Beyond Epistemology"; see Patrice Flichy, *Understanding Technological Innovation*; see Anthony Giddens, *The Constitution of Society*; see Sally Falk Moore, "Law and Social Change"; see Franz von Benda-Beckmann, "Who's Afraid of Legal Pluralism?"

¹⁵ See David Nelken, "Law in action or living law? Back to the beginning in sociology of law"; see David Nelken, "The 'Gap Problem' in the Sociology of Law: A Theoretical Review"; see Roger Cotterrel, *Law's Community*; see Max Travers, *Understanding Law and Society*; see John Griffiths, "The Social Working of Legal Rules"; see David Trubek and John Esser, "Critical Empiricism in American Legal Studies"; see Amir Licht, "Social Norms and the Law: Why Peoples Obey the Law"; see Peer Zumbansen, "Transnational Legal Pluralism".

¹⁶ See Sheila Jasanoff, "Beyond Epistemology"; See Sheila Jasanoff, "Ordering knowledge, ordering society" 15; see Trevor Pinch and Wiebe Bijker, "The Social Construction of Facts and Artefacts"; Helga Nowotny, "How Many Policy Rooms are There?: Evidence-Based and Other Kinds of Science Policies" 480.

¹⁷ See Helen Nissenbaum, "How Computer Systems Embody Values" 120 and 118; see Batya Friedman (ed), *Human Values and the Design of Computer Technology*; see Trevor Pinch and Wiebe Bijker, "The Social Construction of Facts and Artefacts" 428; see Sven Dietrich and others "Ethics in data sharing".

nology and STS scholars should be mindful that the law is not a black box and they too can derive much benefit from studying the complexity, plurality and flexibility of legal systems and processes. Whether the focus is on technology, law, or both, examining the attendant cultures and social practices is vital because it can provide a better understanding of how things work (i.e., what makes them tick and why people act the way they do) and thus lead to more socially-informed and evidence-based approaches and solutions to the problems brought about by socio-technical change.

Understanding the technology is only the first step. To produce more relevant, robust and actionable research findings and recommendations, it would be worthwhile for technology law scholars to conduct research that is grounded on or at least informed by social or empirical data.¹⁸ Assuming the availability of the necessary time and resources and the appropriateness to the aims or goals of their research, technology law scholars should seriously consider engaging in primary empirical research similar to the one undertaken in this book. There are many theories, concepts and research methods in the social sciences and other disciplines that could be profitably applied to studying the social, technical and legal domains not only of hackers but also of many other social groups or fields. Bourdieu's habitus,¹⁹ Giddens's theory of structuration,²⁰ Latour's Actor-Network-Theory,²¹ Luhmann's systems theory,²² Corbin and Strauss's Grounded Theory²³ and Ayres and Braithwaite's responsive regulation²⁴ are just some of

¹⁸ See for example Emilie Cloatre, *Pills for the Poorest: An Exploration of TRIPS and Access to Medication in Sub-Saharan Africa*; see also Julie Cohen, *Configuring the Networked Self*; see also Kathy Bowrey, *Law and Internet Cultures* see also Balazs Bodo, "Coda: A Short History of Book Piracy".

¹⁹ See Pierre Bourdieu, *Outline of a Theory of Practice*.

²⁰ See Anthony Giddens, *The Constitution of Society*.

²¹ See Bruno Latour, *Reassembling the Social*; see Michel Callon "Society in the Making"; see for example Emilie Cloatre, *Pills for the Poorest: An Exploration of TRIPS and Access to Medication in Sub-Saharan Africa*.

²² See Niklas Luhmann, *Law as a Social System*; see for example Andrew Murray, *The Regulation of Cyberspace*.

²³ See Anselm Strauss and Juliet Corbin, "Grounded Theory Methodology: An Overview"; see Kathy Charmaz, *Constructing Grounded Theory*.

²⁴ See Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992) (but with a less state-centric and dyadic approach and a greater focus on third party non-state actors like public interest groups and social movements); see Christine Parker, "Twenty years of responsive regulation: An appreciation and appraisal" 4, 5, 8 and 9; see Peter Grabosky, "Beyond Responsive Regulation: The expanding role of non-state actors in the regulatory process" 114 and 120.

the theories or concepts that technology law scholars could further explore or possibly use. Law and technology researchers can also choose from a wide range of qualitative or quantitative research methods.²⁵ As was done for this book, researchers can interview or hang out with members of a social group or technical community and really get to know their research subjects. More sophisticated and cutting-edge digital tools and data analysis techniques can also be used for legal research, particularly in relation to social networks and social media.²⁶ Of course, conducting primary data collection and analysis may not always be needed or called for. Technology law scholars can also quite easily carry out empirically based or supported research by simply citing or referencing the primary research of other scholars or using existing empirical data in their work.

It is true that undertaking this type of interdisciplinary, socially-informed and empirically-grounded legal research requires significant time, effort and resources. It is quite challenging and time-consuming. Yet, as this book bears out, a socio-techno-legal approach can produce more systematic, rigorous and sensitive research on hackers and hacking and potentially other techno-social fields and activities. By focusing on a research or regulatory subject's practices, technologies, norms and values and their complex and dynamic interactions with law, people can more clearly observe and understand what and whose norms and laws actually regulate and govern behavior in a networked world, and which of these norms and laws need to be broken and remade in light of current and prospective legal, social and technological changes and challenges that society faces.²⁷

²⁵ See Alan Bryman, *Social Research Methods*; Reza Banakar and Max Travers, *Theory and Method in Socio-Legal Research*; Robert Yin, *Case Study Research*; see Balazs Bodo and Zoltan Lakatos, "Theatrical Distribution and P2P Movie Piracy: A Survey of P2P Networks in Hungary Using Transactional Data".

²⁶ See Christine Hine, *Virtual Ethnography*; see Matthew North, *Data Mining for the Masses*; see E. Gabriella Coleman, "Ethnographic Approaches to Digital Media"; see Angela Cora Garcia and others, "Ethnographic Approaches to the Internet and Computer-Mediated Communication"; see Dhiraj Murthy, "Digital Ethnography: An Examination of the Use of New Technologies for Social Research"; see Association of Internet Researchers (AoIR), "Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)".

²⁷ See Michael Dizon, "Rules of a networked society: Here, there and everywhere".

APPENDIX A

Interview guide

Hacking and hacker project

- Do you consider yourself a hacker/Would others call you a hacker? Why or why not?
- For you, what is hacking? How would you define/describe it?
- Of the many technologies and projects that you've worked on, what project are you most proud of? What's your favorite project?
- What does it do? Can you explain how it works?
- Why did you decide to build it? What was your objective or purpose?
- Why did you design it in this way? What did you put in that feature?
- Why was it important?
- What else have you done with this project? What are your plans with it? Why?
- Where and when did you work on it? Who else was involved?
- Have other people seen this? Who were they? What did they say and how did they react?

Norms and values

- What is the purpose/meaning of hacking for you?
- Why do you hack or make? What motivates you?
- Does hacking/making promote any personal or social ethics, goals

or values? Like what? Can you explain?

- (Here's a draft/working list of hacker values that I prepared). For you, which are the 3 most important ones? Can you explain why these are the most significant?
- Are there values that should be added? Are there values that should not be included in this list?
- Do you think that your project supports these values? How? Was it a deliberate or conscious decision on your part?
- Do you think laws conflict with hacker ethics? Any law in particular that in your opinion goes against hacker norms and values?
- What should hackers do when laws restrict/impinge on their norms and values? Can you explain why?
- How about laws that are consistent with hacker ethics? Should hackers do anything with regard to these laws?

Law

- Would you say that law influences what you do? By "law", I mean (for example) computer crime laws, intellectual property laws, contract law, as well as, government policies and regulations.
- In relation to your project, are/were you concerned about legal issues?
- Have there been instances where you stopped or hesitated working on a project because of legal concerns? Can you explain what happened?
- Do you know of other hackers who stopped or changed their projects because of legal issues?
- What do think or feel about the law and authorities? Is the effect of law on hacking positive or negative?
- Have you tried to learn more about the law? How did you do it?
- Do you discuss legal concerns with other hackers in the same way

that you might discuss technical problems? Why/why not?

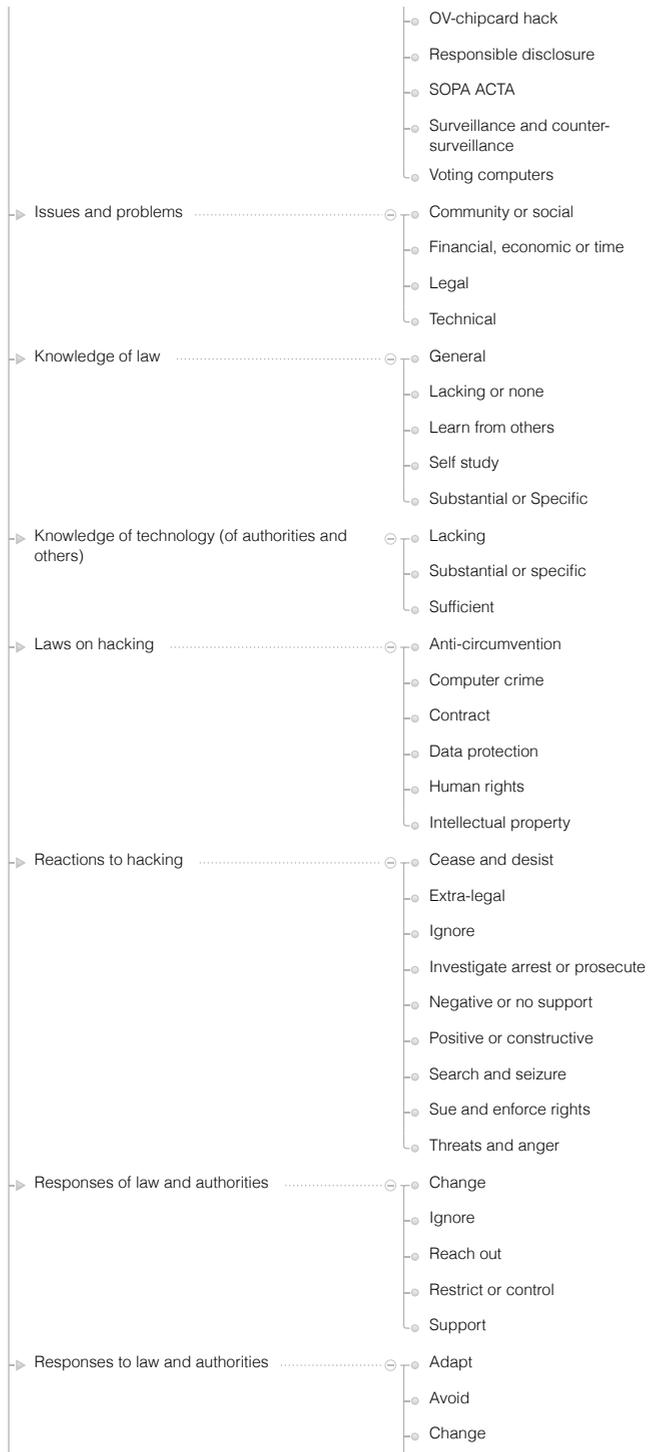
Hacking's interactions with law

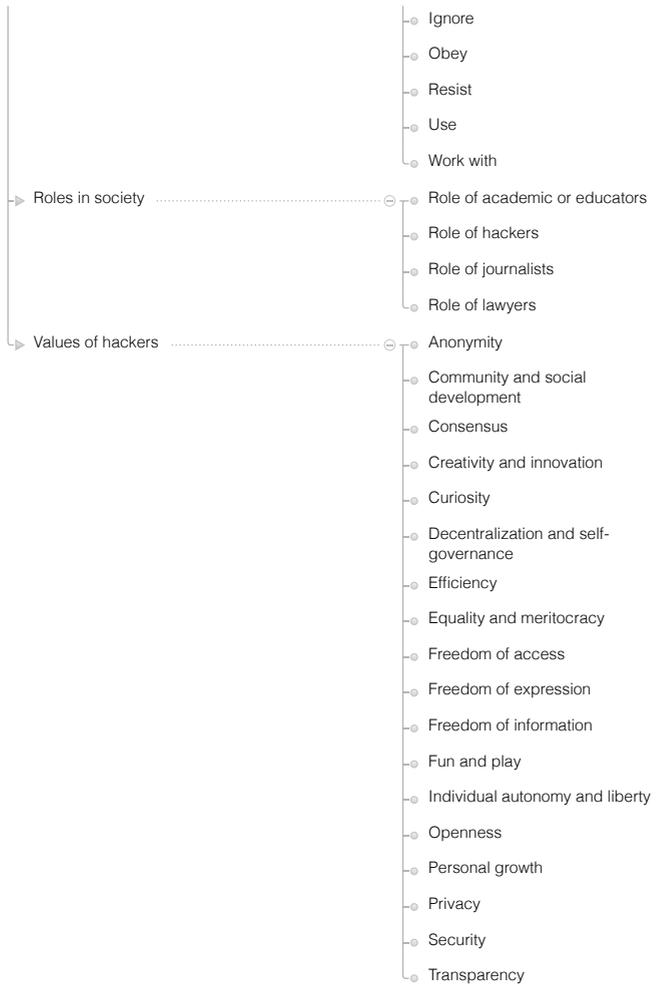
- What is the role of hackers/hacking in society?
- Do you think hacking or hacktivism can change law and public policy?
- Are you familiar with the hacking of the electronic voting machines? Do you have an opinion about it? Do you agree or disagree with the hacktivists' aims and means? What do you think about the outcome? What for you would have been a better solution or best-case scenario?
- Do you know of other cases or instances where hackers or hacking have been in conflict with the law? Can you explain what happened?
- What are your thoughts and feelings about: the OV chipkaart hack, responsible disclosure rules, laws against computer trespass, Leaktobler, government surveillance and counter surveillance projects, open data hackathons, open source and standards, MakerBot closure, 3D printing patent lawsuits, blocking of The Pirate Bay, net neutrality, or other legal and technical issues?

APPENDIX B

Code List







▶ In vivo and uncategorized codes

- 3D printing
- Access to a lawyer
- Accessibility and availability
- Accomplishment (sense of)
- Activism
- Affordances and neutrality of technology
- Agency and power
- Anarchist
- Anti-capitalist
- Anti-establishment
- Art and beauty
- Authority
- Cannot regulate or control

- CCC
- Challenging
- Change your life
- Cheaper to do
- Co-opted
- Commercial or commercialism
- Communication or connection
- Communist
- Competition issues
- Conflict between law and hacking
- Conflict of norms and values
- Contribute
- Control
- Crime or criminality
- Crowdfunding
- Cyber attack
- Dangerous or heavy
- Defer to law
- Defiant
- Democracy or democratic
- Diversity
- Does not work
- Don't worry about law
- Environmental concern
- Ethics or morality
- Fairness or justice
- Fear of technology
- Find our own way
- Food and technology
- For myself or scratch own itch
- Formality structure or control
- Goal oriented
- Got bought out or sold out
- Hackable
- Hacker
- Hacker and artist
- Hacker and craftsman
- Hacker and security researcher
- Hacker camp or con
- Hacker culture or scene
- Hacker ethics

- Hacker name does not matter
- Hacker name matters
- Hackerspace
- Hackerspace and hacklab
- Hackerspace or fablab
- Hacktivism
- Hands-on imperative
- Hang out
- Hobby
- How it works
- Ideological
- Improve
- Inclusiveness
- Informal
- Interest and fascinated
- Internet
- Law enforcement
- Law vs social norms
- Law vs technology
- Lawless
- Legality of hacking
- Level of commitment
- Libertarian
- Make a difference
- Make people think or be aware
- Maker
- Maker movement
- Male dominated or gender equality
- Marketing and publicity only
- Marxist
- Mathematical
- Meaning of hacking
- Meaning of law
- National security
- Negative public perception
- Netherlands
- Network
- No closure or boundaries
- No pressure or competition
- No responsibility
- No secrecy

- Non-commercial
- Non-financial
- Not anti-establishment
- Not damage or cause harm
- Not dangerous or heavy
- Not democratic
- Not effective enough
- Not everyone can be a maker or hacker
- Not illegal or criminal
- Not interested
- Not just technology
- Not political
- Not pushing hard enough
- Not sue or jail
- Paradox or paradoxical
- Philosophy or philosophical
- Political
- Professionals or middle class
- Projects
- Protest or civil disobedience
- Public debate and awareness
- Public order and safety
- Radical
- Rational or reasonable
- Real and virtual (both needed)
- Rebellious
- Regulate (when or how)
- Responsibility
- Reuse and recycle
- Revolution or revolutionary
- Rules of the game
- Scare government
- Scientific rules or principles
- Self-effacing
- Shyness
- Smart
- Social recognition and acceptance
- Squat
- Sue state or company
- Tactics
- Technical solution

- Teenager
- Tinker
- Too extreme or extremist
- Unpredictable or unforeseeable
- Usability or usefulness
- Void warranty
- Whistleblowing and leaks
- Winners
- Work
- Work alone

BIBLIOGRAPHY

- 3D Hubs Blog, “Open Source 3D Printers stand up to giants Stratasys and 3D Systems” blog.3dhubs.com/post/66187555251/open-source-3d-printers-stand-up-to-giants-stratasys accessed 27 November 2013
- Access to Knowledge, <http://www.cptech.org/a2k/> accessed 12 August 2013
- Abelson H, Ledeen K and Lewis HR, *Blown to Bits: Your Life, Liberty and Happiness after the Digital Explosion* (Addison-Wesley 2008)
- Akester P and Akester R, “Digital rights management in the 21st century” (2006) 28 *European Intellectual Property Review* 159
- Alleyne B, “‘We are all hackers now’: critical sociological reflections on the hacking phenomenon” Goldsmiths Research Online <http://eprints.gold.ac.uk/6305/> accessed 2 October 2012
- Altman M, “Hacking at the Crossroad: US Military Funding of Hackerspaces” (2012) *Journal of Peer Production Issue #2*
- Alvarez N and Stephenson J, “A Manifesto for Manifestos” (2012) 150 *Canadian Theatre Review* 3
- Anderson C, *Makers: The New Industrial Revolution* (Random House Business Books 2012)
- Anderson Chris, “The New MakerBot Replicator Might Just Change Your World” wired.com/design/2012/09/how-makerbots-replicator2-will-launch-era-of-desktop-manufacturing/all/ accessed 24 September 2012
- Anonymous, “An Anonymous Manifesto” anonnews.org/press/item/199/ accessed 17 July 2013

- Ante SE, “Skype to Acquire Start-Up GroupMe” <http://www.wsj.com/articles/SB10001424053111903327904576522964260277734> accessed 15 January 2016
- Aoki K, Boyle J and Jenkins J, *Bound by Law?: Tales from the Public Domain* (Center for the Study of the Public Domain 2006)
- Appetas, <http://www.appetas.com/> accessed on 15 January 2016
- Arduino, <http://www.arduino.cc/> accessed 30 August 2013
- Arduino, “Frequently Asked Questions” arduino.cc/en/Main/FAQ accessed 30 August 2013
- Arduino, “What is Arduino?” <https://www.arduino.cc/en/Guide/Introduction> accessed 12 February 2016
- Artisan’s Asylum, “Make a Makerspace” artisansasylum.com/?page_id=2555 accessed 9 February 2013
- Assange J and others, *Cypherpunks: Freedom and the Future of the Internet* (OR Books 2012)
- Association of Internet Researchers (AoIR), “Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)” <http://aoir.org/reports/ethics2.pdf> accessed 12 February 2016
- Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)
- Baichtal J, “Brazilian 3D Printer Company Weighs in on the Makerbot controversy” <http://makezine.com/2012/10/02/brazilian-3d-printer-company-weighs-in-on-the-makerbot-controversy/> accessed 11 February 2016
- Balkin JM, “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society” (2004) 79 *New York University Law Review* 1
- Bambauer DE and Day O, “The Hacker’s Aegis” (2010) 60 *Emory Law Journal* 1051

- Banakar R and Travers M, "Ethnography and Law: Introduction to Section Two" in Reza Banakar and Max Travers (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005)
- Banakar R and Travers M (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005)
- Band J and Gerafi J, *The Fair Use/Fair Dealing Handbook* (Policy-bandwidth 2013)
- Banzi M, "Fighting for Arduino" <http://makezine.com/2015/03/19/massimo-banzi-fighting-for-arduino/> accessed 5 February 2016
- Bardzell J and others, "Virtual Worlds and Fraud: Approaching cybersecurity in massively multiplayer online games" Digital Games Research Association (DiGRA) 2007 Conference
- Barlow JP, "A Declaration of the Independence of Cyberspace" <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 27 May 2014
- Baumann M and others, *Norms and Values: The Role of Social Norms as Instruments of Value Realisation* (Nomos 2010)
- Bazzichelli T, *Networking: The Net as Artwork* (Digital Aesthetics Research Centre 2009)
- Beall R, "Developing a Coherent Approach to the Regulation of Computer Bulletin Boards" (1986) 7 *Computer/Law Journal* 499
- Beebe B, "An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005" (2008) *University of Pennsylvania Law Review* 549
- Belfiore MP, *The Department of Mad Scientists: How DARPA Is Remaking Our World, from the Internet to Artificial Limbs* (Harper Collins 2010)
- Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006)
- Berners-Lee T, "Aaron is dead" W3C mailing list <https://lists.w3.org/Archives/Public/www-tag/2013Jan/0017.html> accessed 15

February 2016

- Berry, DM, "The Contestation of Code: A preliminary investigation into the discourse of the free/libre and open Source Movements" (2004) 1 *Critical Discourse Studies* 65
- Best K, "The Hacker's Challenge: Active Access to Information, Visceral Democracy and Discursive Practice" (2003) 13 *Social Semiotics* 263
- Best K, "Visceral Hacking or Packet Wanking? The Ethics of Digital Code" (2006) 47 *Culture, Theory & Critique* 213
- Bhattacharjee S and others, "Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions" (2006) 49 *Journal of Law and Economics* 91
- Bijker WE, Hughes TP and Pinch TJ (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (The MIT Press 1987)
- Bits of Freedom, "Internet-freedom Toolbox" <https://www.bof.nl/ons-werk/internetvrijheid-toolbox/> accessed 29 July 2015
- Bits of Freedom "Nieuwsbrief Nr. 6.15" <https://www.bof.nl/live/wp-content/uploads/nieuwsbrief160810.txt> accessed 24 August 2015
- Bits of Freedom, "Onze Successen" <https://www.bof.nl/over-ons/onze-successen/> accessed 18 June 2015
- Bits of Freedom, "Position Paper Netwerkneutraliteit" <https://www.bof.nl/live/wp-content/uploads/Position-Paper-netneutraliteit.pdf> accessed 24 June 2015
- Bits of Freedom, "Translations of Key Dutch Internet Freedom Provisions" <https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/> accessed 18 June 2015
- Bisbjerg NK, "The Manifesto. Negotiating Reality" http://www.avant-gardenet.eu/HAC/studentpapers/bisbjerg_manifesto.pdf accessed 15 February 2016

- Bishop W, "The Choice of Remedy for Breach of Contract" (1985) 14
The Journal of Legal Studies 299
- BloomBecker J, "Computer Crime Update: The view as we exit 1984"
(1984) 7 Western New England Law Review 627
- Board of Procurators General, "Responsible Disclosure (how to deal
with 'ethical' hackers?)" (18 March 2013)
- Bodo B, "Coda: A Short History of Book Piracy" in Joe Karaganis (ed),
Media Piracy in Emerging Economies (Social Science Research
Council 2011)
- Bodo B and Lakatos Z, "Theatrical Distribution and P2P Movie Piracy:
A Survey of P2P Networks in Hungary Using Transactional Data"
(2012) 6 International Journal of Communication 413
- Bonnici JPM, Self-Regulation in Cyberspace (TMC Asser Press 2007)
- Borchers J and Bohne R, "A Personal Design Manifesto" <[fabworkshop.
media.mit.edu/2013/04/09/a-personal-design-manifesto/](http://fabworkshop.media.mit.edu/2013/04/09/a-personal-design-manifesto/)>
accessed 31 May 2013
- Borland J, "Hacker space' movement sought for U.S." <[www.wired.
com/threatlevel/2007/08/us-hackers-moun/](http://www.wired.com/threatlevel/2007/08/us-hackers-moun/)> accessed 3 July
2013
- Bourdieu P, The Field of Cultural Production: Essays on Art and Liter-
ature, Randal Johnson (ed) (Polity Press 1993)
- Bourdieu P, "The Force of Law: Toward a Sociology of the Juridical
Field" (1986) 38 The Hastings Law Journal 805
- Bourdieu P, Outline of a Theory of Practice (Cambridge University
Press 1977)
- Bourdieu P, "The social space and the genesis of groups" (1985) 14
Theory and Society 723
- Bowrey K, Law and Internet Cultures (Cambridge University Press
2005)
- Boyle J, "A manifesto on WIPO and the future of intellectual property"

(2004) 9 Duke Law & Technology Review 2

Boyle J, *The Public Domain: Enclosing the Commons of the Mind* (Yale University Press 2008)

Boyle J, *Shamans, Software, and Spleens: Law and the Construction of the Information Society* (Harvard University Press 1996)

Bozeman B and Sarewitz D, "Public Value Mapping and Science Policy Evaluation" (2011) 49 *Minerva* 1

Bradshaw S, Bowyer A and Haufe P, "The Intellectual Property Implications of Low-Cost 3D printing" (2010) 7 *SCRIPTed* 5

Brand S, *The Media Lab: Inventing the Future at MIT* (Penguin Books 1988)

Brand S, "SPACEWAR: Fanatic Life and Symbolic Death Among the Computer Bums" *Rolling Stone* (1972)

Brewster T, "US cybercrime law being used to target security researchers" <http://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers> accessed 9 June 2014

Brocius C, "The Hardware Hacker Manifesto" daeken.com/the-hardware-hacker-manifesto accessed 17 July 2013

Brown I, "The Evolution of Anti-Circumvention Law" (2006) 20 *International Review of Law, Computers & Technology* 239

Brownsword R, "Code, control, and choice: why East is East and West is West" (2005) 25 *Legal Studies* 1

Bryman A, *Social Research Methods* (Oxford University Press 2012)

Bugcrowd, "The Bug Bounty List", <https://bugcrowd.com/list-of-bug-bounty-programs/> accessed 13 August 2015

Callon M, "Society in the Making: The Study of Technology as a Tool for Sociological Analysis" in WE Bijker, TP Hughes and TJ Pinch (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (The MIT Press 1987)

- Cangialosi C, "The Electronic Underground: Computer Piracy and Electronic Bulletin Boards" (1989) 15 Rutgers Computer & Technology Law Journal 265
- Casellati AM, "The Evolution of Article 6.4 of the European Information Society Copyright Directive" (2000) 24 Columbia-VLA Journal of Law & the Arts 369
- Castells M, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001)
- Cavalcanti G, "Is it a Hackerspace, Makerspace, TechShop or Fab-Lab?" <http://makezine.com/2013/05/22/the-difference-between-hackerspaces-makerspaces-techshops-and-fablabs/> accessed 11 February 2016
- Caws MA (ed), *Manifesto: A Century of isms* (University of Nebraska Press 2001)
- Chaos Computer Club, "hackerethics" <http://www.ccc.de/hackerethics> accessed 17 July 2013
- Chadwick, A, *Internet Politics: States, Citizens, and New Communication Technologies* (Oxford University Press 2006)
- Chandler JA, "Security in Cyberspace: Combatting Distributed Denial of Service Attacks" (2004) 1 University of Ottawa Law & Technology Journal 231
- Charmaz K, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis* (SAGE Publications 2006)
- Cho A, "University Hackers Test the Right To Expose Security Concerns" (2008) 322 Science 1322
- Chung CY, "The Computer Fraud and Abuse Act: How Computer Science Can Help With the Problem of Overbreadth" (2010) 24 Harvard Journal of Law & Technology 233
- Cloatre E, *Pills For The Poorest: An Exploration of TRIPS and Access to Medication In Sub-Saharan Africa* (Palgrave Macmillan 2013)

- Cohen JE, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012)
- Cohen JE, “A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace” (1995) 28 *Connecticut Law Review* 981
- Cohn C and Hoffman M, “Rebooting Computer Law Part 2: Protect Tinkerers, Security Researchers, Innovators, and Privacy Seekers” <https://www.eff.org/deeplinks/2013/02/rebooting-computer-crime-law-part-2-protect-tinkerers-security-researchers> accessed 11 February 2016
- Cohn C and Fakhoury H and Hoffman M, “Rebooting Computer Law Part 3: The Punishment Should Fit the Crime” <https://www.eff.org/deeplinks/2013/02/rebooting-computer-crime-part-3-punishment-should-fit-crime> accessed 11 February 2016
- Coldewey D, “The User’s Manifesto” <http://techcrunch.com/2010/04/18/the-users-manifesto-in-defense-of-hacking-modding-and-jailbreaking/> accessed 23 April 2014
- Coleman EG, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton University Press 2013)
- Coleman EG, “Ethnographic Approaches to Digital Media” (2010) 39 *Annual Review of Anthropology* 487
- Coleman EG and Golub A, “Hacker practice: Moral genres and the cultural articulation of liberalism” (2008) 8 *Anthropological Theory* 255
- Coleman EG, “Anonymous: From the Lulz to Collective Action” mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action accessed 22 August 2013
- Coleman, G, “Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers” (2009) 24 *Cultural Anthropology* 420
- Coleman G, “The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld” (2010) 83 *Anthropological Quarterly* 47

- Coleman G, "Hacker Politics and Publics" (2011) 23 *Public Culture* 511
- Computer Desktop Encyclopedia <http://lookup.computerlanguage.com/host_app/search?cid=C999999&def=6861636b-6174686f6e.htm> accessed 20 August 2013
- Computer History Museum, "PDP-1 Restoration Project" <<http://www.computerhistory.org/pdp-1/>> accessed 12 February 2016
- Conrad J, "Seeking help: the important role of ethical hackers" (2012) 8 *Network Security* 5
- Constant SA, "Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare – The Case Against Aaron Swartz and the Need To Reform the CFAA" (2013) 16 *Tulane Journal of Technology and Intellectual Property* 231
- Cooter R, "Normative Failure Theory of Law" (1997) 82 *Cornell Law Review* 947
- Cotterrell R, *Law's Community: Legal Theory in Sociological Perspective* (Oxford University Press 1995)
- Crang M and Cook I, *Doing Ethnographies* (SAGE Publications 2007)
- Creative Commons Corporation, "Defining 'Noncommercial': A Study of How the Online Population Understands 'Noncommercial Use'" (2009)
- Cringely RX, *Accidental Empires: How the boys of Silicon Valley make their millions, battle foreign competition, and still can't get a date* (Penguin Books 1993)
- Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Autonomedia and Critical Art Ensemble 1996)
- Curcuru S, "An Apache Way Primer" <<http://theapacheway.com/>> accessed 14 February 2013
- Curry-Sumner I and others, *Research Skills: Instruction for Lawyers* (Ars Aequi Libri 2010)

- Data.gov, <http://www.data.gov/> accessed 21 August 2013
- Data.gov.uk, <http://data.gov.uk/about-us> accessed 21 August 2013
- Data.gouv.fr, <http://www.data.gouv.fr/> accessed 21 August 2013
- Data.overheid.nl, <https://data.overheid.nl/> accessed 21 August 2013
- de Haan J, “The New Dutch Law on Euthanasia” (2002) 10 *Medical Law Review* 57
- de Haes AU, “KPN luistert abonnees af met Deep Packet Inspection” <http://webwereld.nl/beveiliging/53691-kpn-luistert-abonnees-af-met-deep-packet-inspection> accessed 18 June 2015
- de Sousa Santos B, “Law: A Map of Misreading. Toward a Postmodern Conception of Law” (1987) 14 *Journal of Law and Society* 279
- De Werra J, “Moving beyond the Conflict between Freedom of Contract and Copyright Policies: In Search of a New Global Policy for Online Information Licensing Transactions – A Comparative Analysis between US Law and European Law” (2003) 25 *Columbia Journal of Law & the Arts* 239
- de Winter B, “Lektoker superknaller: Megalek treft 50 gemeenten” <http://webwereld.nl/beveiliging/54950-lektoker-superknaller-megalek-treft-50-gemeenten> accessed 16 June 2015
- “The Declaration of the Independence of the people of the Internet” http://files.gendo.nl/media/Pirate_declaration_of_Independence_2_printable.pdf accessed 26 August 2013
- Denison DC, “Reactions to the MakerBot-Stratasys Deal” <http://makezine.com/2013/06/20/reactions-to-the-makerbot-stratasys-deal/> accessed 11 February 2016
- Denmead K, “MakerBot Origins: The Revolution Will Be Squirted” <http://makezine.com/2013/06/20/makerbot-origins-the-revolution-will-be-squirted/> accessed 11 February 2016
- Denmead, Ken. “Why the Maker Movement is Here to Stay” <http://makezine.com/2013/06/03/why-the-maker-movement-is-here-to-stay/> accessed 11 February 2016

- Determann L, "Internet Freedom and Computer Abuse" (2012) 35 Hastings Communications & Entertainment Law Journal 429
- Dietrich S and others, "Ethics in data sharing: developing a model for best practice" IEEE Security and Privacy Workshops 2014
- Dizon MAC, "Decompiling the Software Directive, the Microsoft CFI case and the I2010 strategy: How to reverse engineer an international interoperability regime" (2008) 14 Computer and Telecommunications Law Review 213
- Dizon MAC, "Does Technology Trump Intellectual Property?: Re-framing the Debate About Regulating New Technologies" (2011) 8 SCRIPTed 124
- Dizon MAC, "Free and Open Source Software Communities, Democracy and ICT Law and Policy" (2010) 18 International Journal of Law and Information Technology 127
- Dizon MAC, "Law and Networks: Legal Pluralism in Information and Communications Technology (2011) 15 Journal of Internet Law 1
- Dizon MAC, "Participatory Democracy and Information and Communications Technology: A Legal Pluralist Perspective" (2010) European Journal of Law and Technology Vol. 1 Issue 3
- Dizon MAC, "The Symbiotic Relationship Between Global Contracts and the International IP Regime" (2009) 4 Journal of Intellectual Property Law & Practice 559
- Dizon MAC, "Rules of a networked society: Here, there and everywhere" in R Leenes and E Kosta (eds), Bridging Distances in Technology and Regulation (Wolf Legal Publishers 2013)
- Doctor Crash, "The Techno-Revolution" Phrack <<http://phrack.org/issues/6/3.html>> accessed 4 July 2013
- Doctorow C, "Lockdown: The Coming War on General-purpose Computing" Boing Boing <boingboing.net/2012/01/10/lockdown.html> accessed 24 June 2013
- Dohrenwend BP, "Egoism, Altruism, Anomie, and Fatalism: A Concep-

tual Analysis of Durkheim's Types" (1959) 24 American Sociological Review 466

Dougherty D, "From Hackers to Makers" <<http://summit.oshwa.org/files/2012/07/From-Hackers-to-Makers.pdf>> accessed 19 October 2012

Doyle C, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service 2010)

Drahos P, "Bilateralism in Intellectual Property" (Oxfam 2001)

Drahos P and Braithwaite J, *Information Feudalism* (Earthscan Publications 2002)

Dryzek, JS, "Liberal Democracy and the Critical Alternative" in *Deliberative Democracy and Beyond: Liberals, Critics, Contestations* (Oxford University Press 2002)

Dusollier S, "Exceptions and Technological Measures in the European Copyright Directive of 2001 - An Empty Promise" (2003) 34 *International Review of Intellectual Property and Competition Law* 62

Dyson G, *Turing's Cathedral: The Origins of the Digital Universe* (Random House Audio 2012)

Easterbrook FH, "Cyberspace and the Law of the Horse" (1996) *University of Chicago Legal Forum* 207

Easy Taxi, <<http://www.easytaxi.com/>> accessed on 15 January 2016

Ebert TL, "Manifesto as Theory and Theory as Material Force: Toward a Red Polemic" (2003) 23 *JAC* 553

Edwards K, "Epistemic Communities, Situated Learning and Open Source Software Development" <http://orbit.dtu.dk/fedora/objects/orbit:51813/datastreams/file_2976336/content> accessed 8 November 2012

Electronic Frontier Foundation, "In the Wake of Aaron Swartz's Death, Let's Fix Draconian Computer Crime Law" <<https://www.eff>

org/deeplinks/2013/01/aaron-swartz-fix-draconian-computer-crime-law› accessed 12 February 2016

Electronic Frontier Foundation, “Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems” (February 2011)

Electronic Frontier Foundation, “Surveillance Self-Defense” (<https://ssd.eff.org/en>) accessed 29 July 2015

Electronic Frontier Foundation, “Unintended Consequences: Fifteen Years under the DMCA” (March 2013) (<https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca>) accessed 12 February 2016

Elkin-Koren N, “Copyright Policy and the Limits of Freedom of Contract” (1997) 12 Berkeley Technology Law Journal 93

Elkin-Koren N, “Exploring Creative Commons” in PB Hugenholtz and L Guibault (eds) *The Future of the Public Domain* (Kluwer Law International 2006)

Ellickson RC, “The Evolution of Social Norms: A Perspective from the Legal Academy” (1999) Yale Law School, Program for Studies in Law, Economics and Public Policy, Working Paper 230

Ellickson, RC, *Order Without Law: How Neighbors Settle Disputes* (Harvard University Press 1991)

Elliot MS and Scacchi W, “Mobilization of software developers: the free software movement” (2008) 21 *Information Technology & People* 4

Eschenfelder KR and Desai AC, “Software as Protest: The Unexpected Resiliency of U.S.-Based DeCSS Posting and Linking” (2004) 20 *The Information Society* 101

Eschenfelder KR, Howard RG and Desai AC, “Who Posts DeCSS and Why?: A Content Analysis of Web Sites Posting DVD Circumvention Software” (2005) 56 *Journal of the American Society for Information Science and Technology* 1405

Essers L, “Dutch government aims to shape ethical hackers’ disclosure practices” http://www.pcworld.idg.com.au/article/445591/dutch_government_aims_shape_ethical_hackers_disclosure_practices/ accessed 11 February 2016

Etzioni A, “Social norms: Internalization, Persuasion, and History” (2000) 34 *Law & Society Review* 157

European Commission, “Questions and Answers: Directive on attacks against information systems” MEMO/13/661, 4 July 2013

European Commission, “Report based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information system” COM(2008) 444, 14 July 2008

European Commission, “Report on the application of the Directive 2001/29/EC” SEC(2007) 1556

European Commission, “Staff Working Paper Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive amending Directive 2003/98/EC on the re-use of public sector information”

European Patent Office, “Patents for software? European law and practice” <http://www.epo.org/news-issues/issues/software.html> accessed 24 July 2015

Europeana, “Hackathons” <http://pro.europeana.eu/web/guest/hackathon-prototypes> accessed 21 August 2013

Evans C, “Announcing Project Zero” <http://googleprojectzero.blogspot.nl/2014/07/announcing-project-zero.html> accessed 16 July 2014

“The Fab Charter”, fab.cba.mit.edu/about/charter/ accessed 15 August 2013

Farnsworth EA, “Legal Remedies for Breach of Contract” (1970) 70 *Columbia Law Review* 1145

Farr N, “Respect the Past, Examine the Present, Build the Future” blog.hackerspaces.org/2009/08/25/respect-the-past-examine-the-present-build-the-future/ accessed 3 July 2013

- Farr N, “The Rights and Obligations of Hackerspace Members” <blog.hackerspaces.org/2009/08/19/rights-and-obligations-of-hackerspace-members/> accessed 15 August 2013
- Fakhoury H, “The U.S. Crackdown on Hackers Is Our New War on Drugs” <http://www.wired.com/opinion/2014/01/using-computer-drug-war-decade-dangerous-excessive-punishment-consequences/> accessed 24 January 2014
- Fauteux B, “‘New Noise’ versus the Old Sound: Manifestos and The Shape of Punk to Come” (2012) 35 *Popular Music and Society* 465
- Feenberg A, “Democratizing Technology: Interest, Codes, Rights” (2001) 5 *The Journal of Ethics* 177
- Feenberg A, “Escaping the Iron Cage, or, Subversive Rationalization and Democratic Theory” in R Schomberg (ed), *Democratizing Technology: Theory and Practice of Deliberative Technology Policy* (International Centre for Human and Public Affairs 1999)
- Fine G, “Enacting Norms: Mushrooming and the Culture of Expectations and Explanations” in M Hechter and KD Opp (eds), *Social Norms* (The Russell Sage Foundation 2001)
- Fisher E and others, “The Public Value of Nanotechnology?” (2010) 85 *Scientometrics* 29
- Flichy P, *Understanding Technological Innovation: A Socio-Technical Approach* (Edward Elgar 2007)
- Flood J, “Socio-Legal Ethnography” in R Banakar and M Travers (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005)
- Frack, <http://frack.nl/> accessed 21 August 2013
- France AK, “In The Shed: Shiny! New! Ultimaker 2!” <http://makezine.com/2013/12/06/in-the-shed-shiny-new-ultimaker-2/> accessed 11 February 2016
- “The Free Software Definition” <http://www.gnu.org/philosophy/free-

sw.html accessed 2 July 2013

Free Software Foundation, "What is free software" <<http://www.gnu.org/philosophy/free-sw.html>> accessed 7 November 2012

Freitas PMF and Gonçalves N, "Illegal access to information systems and the Directive 2013/40/EU" (2015) 29 *International Review of Law, Computers & Technology* 50

Friedman B (ed), *Human Values and the Design of Computer Technology* (Cambridge University Press 1997)

Friedman B and Nissenbaum H, "Bias in Computer Systems" (1996) 14 *ACM Transactions on Information Systems* 330

Friese, S, *Qualitative Data Analysis with ATLAS.ti* (SAGE Publications 2014)

Galbraith, CD, "Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites" (2004) 63 *Maryland Law Review* 320

Galligan DJ, *Law in Modern Society* (Oxford University Press 2007)

Garcia, AC and others, "Ethnographic Approaches to the Internet and Computer-Mediated Communication" (2009) 38 *Journal of Contemporary Ethnography* 52

Gates B, "Open Letter to Hobbyists" <https://upload.wikimedia.org/wikipedia/commons/1/14/Bill_Gates_Letter_to_Hobbyists.jpg> accessed 7 February 2013

Gasser U and Ernst S, "From Shakespeare to DJ Danger Mouse: A Quick Look at Copyright and User Creativity in the Digital Age" Berkman Center for Internet & Society Research Publication No. 2006-05

Gasser U and Girsberger M, "Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States - A Genie Stuck in the Bottle?" Berkman Center for Internet & Society Research Publication No. 2004-10

Gehling R, Ashley CR and Griffin T, "Electronic Emissions Security:

- Danger in the Air” (2007) 24 *Information Systems Management* 305
- Geiger C, “The answer to the machine should not be the machine: safeguarding the private copy exception in the digital Environment” (2008) 30 *European Intellectual Property Review* 121
- Geiger C, Gervais D and Senffleben M, “The Three-Step Test Revisited: How to Use the Test’s Flexibility in National Copyright Law” (2013) 29 *American University International Law Review* 581
- Gerschenfeld, N, “How to Make Almost Anything: The Digital Fabrication Revolution” (2012) 91 *Foreign Affairs* 43
- Gervais DJ, “Making Copyright Whole: A Principled Approach to Copyright Exceptions and Limitations” (2008) 5 *University of Ottawa Law & Technology Journal* 1
- Gibbons LJ, “No Regulation, Government Regulation, or Self-regulation: Social Enforcement or Social Contracting for Governance in Cyberspace” (1997) 6 *Cornell Journal of Law and Public Policy* 475
- Gibbs JP, *Norms, Deviance, and Social Control: Conceptual Matters* (Elsevier 1981)
- Gibbs JP, “Norms: The Problem of Definition and Classification” (1965) 70 *American Journal of Sociology* 586
- Gibbs JP. “The Sociology of Law and Normative Phenomena” (1966) 31 *American Sociological Review* 315
- Giddens A, *The Constitution of Society: Outline of the Theory of Structuration* (Polity Press 1984)
- Giddens, A, *Sociology* (Polity Press 2009)
- Gillen M, “Human versus Inalienable Rights: Is there still a future for online protest in the Anonymous world?” (2012) *European Journal of Law and Technology* Vol. 3 No. 1
- Ginsburg JC, “Copyright and Control Over New Technologies of Dissemination” (2001) 101 *Columbia Law Review* 1613

- Giseburt R, “Is One of Our Open Source Heroes Going Closed Source?” blog.makezine.com/2012/09/19/is-one-of-our-open-source-heroes-going-closed-source/ accessed 24 September 2012
- Giseburt R, “MakerBot’s Mixed Messages About Open Source, Their Future” <http://makezine.com/2012/09/22/makerbots-mixed-messages-about-open-source-their-future/> accessed 11 February 2016
- GNU Emacs General Public License, www.free-soft.org/gpl_history/emacs_gpl.html accessed 8 August 2013
- “GNU General Public License version 1”, www.gnu.org/licenses/gpl-1.0-standalone.html accessed 25 April 2012
- Goldsmith J, “Regulation of the Internet: Three Persistent Fallacies” (1998) 73 Chicago-Kent Law Review 1119
- Goldsmith J and Wu T, Who Controls the Internet?: Illusions of a Borderless World (Oxford University Press 2006)
- Gonggrijp R and Hengeveld W, “Studying the Nedap/Groenendaal ES3B voting computer” <http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf> accessed 11 February 2016
- Good T, “What is ‘Making?’” <http://makezine.com/2013/01/28/what-is-making/> accessed 15 February 2016
- Google, “Crawling & Indexing” <http://www.google.com/intl/en/insidesearch/howsearchworks/crawling-indexing.html> accessed 21 August 2014
- Gordon D, “Forty Years of Movie Hacking: Considering the Potential Implications of the Popular Media Representation of Computer Hackers from 1968 to 2008” (2010) 2 International Journal of Internet Technology and Secured Transactions 59
- Government of the Netherlands, “Guidelines for responsible disclosure of IT vulnerabilities” www.government.nl/news/2013/01/03/guideline-for-responsible-disclosure-of-it-vulnerabilities.html accessed 21 August 2013

- Graboksy P, "Beyond Responsive Regulation: The expanding role of non-state actors in the regulatory process" (2013) 7 *Regulation & Governance* 114
- Graham P, *Hackers & Painters: Big Ideas from the Computer Age* (O'Reilly Media 2004)
- Greenberg A, "Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers" <http://www.wired.com/2014/07/google-project-zero/> accessed 16 July 2014
- Greenwald G, "The inspiring heroism of Aaron Swartz" www.theguardian.com/commentisfree/2013/jan/12/aaron-swartz-heroism-suicide1/print accessed 26 August 2013
- Grenzfurthner J and Schneider FA, "Rewriting Hacking the Spaces" hackerspaces.org/wiki/rewriting_Hacking_the_Spaces accessed 3 July 2013
- Griffith A, "Legal Pluralism" in R Banakar and M Travers (eds), *An Introduction to Law and Social Theory* (Hart Publishing 2002)
- Griffiths J, "The Social Working of Legal Rules" (2003) 48 *Journal of Legal Pluralism* 1
- Griffiths J, "What is Legal Pluralism?" (1986) 24 *Journal of Legal Pluralism* 1
- GroupMe, <https://groupme.com/> accessed 15 January 2016
- Guadamuz A, "The Software Patent Debate" (2006) 1 *Journal of Intellectual Property Law & Practice* 196
- Guibault L, Westkamp G and Rieber-Mohn T, "Study on the Implementation and Effect in Member States' Laws on Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society" Amsterdam Law School Legal Studies Research Paper No. 2012-28
- Gunkel DJ, "Editorial: introduction to hacking and hacktivism" (2005) 7 *New Media & Society* 595
- "GURPS Cyberpunk" <http://www.sjgames.com/gurps/books/cyber->

punk/› accessed 28 April 2014

HackerOne, “Vulnerability Disclosure Guidelines” (<https://hackerone.com/disclosure-guidelines>) accessed 13 August 2015

Hackerspace Open Day (<https://revspace.nl/HackerspaceDagEn2012>) accessed on 27 March 2013

Hackerspaces – The Beginning (2011) (<http://archive.org/details/hackerspaces-the-beginning>) accessed 2 October 2012

Hackerspaces.nl, (<http://hackers.nl>) accessed on 12 November 2015

Hackerspaces.org, (<http://hackerspaces.org/wiki/>) accessed on 15 August 2013

Hafner K and Lyon M, *Where Wizards Stay Up Late: The Origins of the Internet* (Simon & Schuster 1996)

Hahn R, “Government Policy toward Open Source Software: An Overview” (http://www.brookings.edu/press/books/chapter_1/governmentpolicytowardopensourcesoftware.pdf) accessed 11 February 2016

Halbert D, “Discourses of Danger and the Computer Hacker” (1997) 13 *The Information Society* 361

Halbert D, “Mass Culture and the Culture of the Masses: A Manifesto for User-Generated Rights” (2009) 11 *Vanderbilt Journal of Entertainment & Technology Law* 921

Hampson NCN, “Hacktivism: A New Breed of Protest in a Networked World” (2012) 35 *Boston College International and Comparative Law Review* 511

Hart RJ, “Interoperability information and the Microsoft decision” (2006) 28 *European Intellectual Property Review* 361

Hart RJ, “Interfaces, interoperability and maintenance” (1991) 13 *European Intellectual Property Review* 111

Hart SL, “Axiology – Theory of Values” (1971) 32 *Philosophy and Phenomenological Research* 29

- Hatch M, *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers* (McGraw Hill Professional 2013)
- Hayek, FA, *Law, Legislation and Liberty: Volume I Rules and Order* (The University of Chicago Press 1973)
- Hechter M, “Should Values Be Written Out of the Social Scientist’s Lexicon” (1992) 10 *Sociological Theory* 214
- Hechter M and Opp KD (eds), *Social Norms* (The Russel Sage Foundation 2001)
- Higgins P, “Critical Fixes for the Computer Fraud and Abuse Act” <https://www.eff.org/deeplinks/2013/01/these-are-critical-fixes-computer-fraud-and-abuse-act> accessed 11 February 2016
- Higgins P, “The Netherlands Passes Net Neutrality Legislation” <https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation> accessed 18 June 2015
- Himanen P, “A Brief History of Computer Hackerism” in *The Hacker Ethic and the Spirit of the Information Age* (Secker & Warburg 2001)
- Himanen P, *The Hacker Ethic and the Spirit of the Information Age* (Secker & Warburg 2001)
- Himma, KE, “Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?” <http://dx.doi.org/10.2139/ssrn.799545> accessed 11 February 2016
- Hine C, “How Can Qualitative Internet Researchers Define the Boundaries of Their Projects?” in AN Markham and NK Baym (eds), *Internet inquiry: Conversations about method* (Sage 2009)
- Hine, Christine. “Virtual Ethnography” <http://www.cirst.uqam.ca/PCST3/PDF/Communications/HINE.PDF> accessed 15 February 2016
- Hitlin S and Piliavin JA, “Values: Reviving a Dormant Concept” (2004) 30 *Annual Review of Sociology* 359

- Hofman M and Reitman R, "Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service" <<https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service>> accessed 11 February 2016
- Hollinger RC, "Computer Crime" <http://users.clas.ufl.edu/rhollin/Computer_Crime.pdf> accessed 15 February 2016
- Hollinger RC, "Hackers: Computer Heroes or Electronic Highwaymen?" (1991) 21 *Computers & Society* 6
- Hollinger RC and Lanza-Kaduce L, "The Process of Criminalization: The Case of Computer Crime Laws" (1988) 26 *Criminology* 101
- Holmes, Jr, OW, "Privilege, Malice, and Intent" (1894) *Harvard Law Review* 1
- Horne C, "Sociological Perspectives on the Emergence of Social Norms" in M Hechter and KD Opp (eds), *Social Norms* (The Russel Sage Foundation 2001)
- Hugenholtz PB and Okediji R, "Conceiving an International Instrument on Limitations and Exceptions to Copyright" Amsterdam Law School Research Paper No. 2012-43
- Hughes E, "A Cypherpunk's Manifesto" <w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto> accessed 17 July 2013
- Huijboom N and Van den Broek T, "Open data: an international comparison of strategies" (2011) 12 *European Journal of ePractice* 1
- Hutchby I, "Technologies, Texts and Affordances" (2001) 35 *Sociology* 441
- iFixit, "Self-Repair Manifesto" <<http://www.ifixit.com/Manifesto>> accessed 27 May 2014
- IKEA hackers <<http://www.ikeahackers.net/>> accessed 16 August 2013
- Instructables, "Arduino Projects" <<http://www.instructables.com/id/Arduino-Projects/>> accessed 12 February 2016

- Interference, “Calling for Papers” <http://interference.io/cfp.php> accessed on 6 May 2014
- Internet Society, “Brief History of the Internet” <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> accessed 20 November 2012
- Iwahashi R, “How to Circumvent Technology Protection Measures Without Violating the DMCA: An Examination of Technological Protection Measures Under Current Legal Standards” (2011) 26 Berkeley Technology Law Journal 491
- Jacobs B, “Architecture Is Politics: Security and Privacy Issues in Transport and Beyond” in S Gutwirth and others (eds) *Data Protection in a Profiled World* (Springer 2010)
- Jacobs B and Pieters W, “Electronic Voting in the Netherlands: from early Adoption to early Abolishment” in A Aldini, G Barthes and R Gorrieri (eds), *Foundations of Security Analysis and Design V* (Springer 2009)
- Jasanoff S, “Beyond Epistemology: Relativism and Engagement in the Politics of Science” (1996) 26 *Social Studies of Science* 393
- Jasanoff S, “Ordering knowledge, ordering society” in S Jasanoff (ed), *States of Knowledge: The Co-Production of Science and the Social Order* (Routledge 2004)
- Jasanoff S, “What Judges Should Know About the Sociology of Science” (1992) 32 *Jurimetrics* 345
- Jensen EC, “An Eletronic Soapbox: Computer Bulletin Boards and the First Amendment” (1987) 39 *Federal Communications Law Journal* 217
- Jensen S, “Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail” (2013) 36 *Hamline Law Review* 81
- Johnson DR and Post D, “Law and Borders - The Rise of Law in Cyberspace” (1996) 48 *Stanford Law Review* 1367
- Jordan T, *Hacking: Digital Media and Technological Determinism* (Pol-

ity Press 2008)

Jordan T, *Activism!: Direct Action, Hacktivism and the Future of Society* (Reaktion books 2002)

Jordan T and Taylor P, "A sociology of hackers" (1998) 46 *The Sociological Review* 757

Kamphuis, A, "Dining with Assange and Spies" www.huffingtonpost.co.uk/arjen-kamphuis/dining-with-julian-assange_b_2565962.html?view=print&comm_ref=false accessed 26 August 2013

Karanasiou AP, "The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Service (DDoS) attacks" (2014) 28 *International Review of Law, Computers & Technology* 98

Katz A, "Towards a Functional Licence for Open Hardware" (2012) *International Free and Open Source Software Law Review* Vol. 4 No. 1

Katz AW, "Remedies for breach of contract under the CISG" (2006) 25 *International Review of Law and Economics* 378

Kelty CM, "Culture's Open Sources: Software, Copyright, and Cultural Critique" (2004) 77 *Anthropological Quarterly* 499

Kelty C, "Geeks, Social Imaginaries, and Recursive Publics" (2005) 20 *Cultural Anthropology* 185

Kelty CM, *Two Bits: The Cultural Significance of Free Software* (Duke University Press 2008)

Kera D, "Hackerspaces and DIYbio in Asia: connecting science and community with open data, kits and protocols" (2012) *Journal of Peer Production* Issue #2

Kerr IR, Maurushat A and Tacit CS, "Technical Protection Measures: Tilting at Copyright's Windmill" (2002-2003) 32 *Ottawa Law Review* 7

Kerr OS, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" (2003) 78 *New York University*

Law Review 1596

Kerr OS, "Vagueness Challenges to the Computer Fraud and Abuse Act" (2010) 94 Minnesota Law Review 1561

"Kickstart Leeuwarden" http://frack.nl/wiki/Kickstart_Leeuwarden accessed 19 November 2012

"Kickstart058 Hackathon" <http://oif058.fikket.com/event/hackathon-kickstart058> accessed 19 November 2012

Kirsch C, "The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law" (2014) 41 Northern Kentucky Law Review 383

Kirtchev, CA, "A Cyberpunk Manifesto" http://project.cyberpunk.ru/idb/cyberpunk_manifesto.html accessed 27 May 2014

Klang M, "Civil Disobedience Online" (2004) 2 Journal of Information, Communication and Ethics in Society 75

Kluckhohn C and others, "Values and Value-Orientations in the Theory of Action" in T Parsons and EA Shils (eds), *Toward a General Theory of Action* (Harper Torchbooks 1951)

Knobel C and Bowker GC, "Values in Design" (2011) 54 Communications of the ACM 26

Koops B, "Cybercrime Legislation in the Netherlands" International Congress on Comparative Law 2010

Koops B, "Ten dimensions of technology regulation – Finding Your Bearings in the Research Space of an Emerging Discipline" Tilburg University Legal Studies Working Paper Series No. 015/2010

Kreimer SF, "Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet" (2001) 150 University of Pennsylvania Law Review 119

Kroker ER, "The Computer Directive and the balance of rights" (1997) 19 European Intellectual Property Review 247

Kurutz S, "One Big Workbench" The New York Times www.nytimes.

com/2013/05/02/garden/the-rise-of-the-hacker-space.html?pagewanted=all&_r=1&&pagewanted=print accessed 17 May 2013

Langman L, "From Virtual Public Spheres to Global Justice: A Critical Theory of Interneted Social Movements" (2005) 23 *Sociological Theory* 42

Lapsley P, "The Definitive Story of Steve Wozniak, Steve Jobs, and Phone Phreaking" *The Atlantic* (20 February 2013)

Lapsley P, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (Audible 2013)

Latour B, "Give Me a Laboratory and I will Raise the World" in KD Knorr-Cetina and M Mulkay (eds), *Science Observed: Perspectives on the Social Study of Science* (Sage Publications 1983)

Latour B, *Reassembling the Social – An Introduction to Actor-Network-Theory* (Oxford University Press 2005)

Latour B and Woolgar S, *Laboratory Life: The Construction of Scientific Facts* (Princeton University Press 1986)

Layton R, "Net neutrality in the Netherlands: Dutch solution or Dutch disease?" 24th European Regional Conference of the International Telecommunication Society 2013

Lee GK and Cole RE, "From a Firm-Based to a Community-Based Model of Knowledge Creation: The Case of the Linux Kernel Development" (2003) 14 *Organizational Science* 633

Leenes R, "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology" (2011) 5 *Legisprudence* 143

Lerner J and Tirole J, "The Economics of Technology Sharing: Open Source and Beyond" (2005) 19 *The Journal of Economic Perspectives* 99

Lessig L, *Code and Other Laws of Cyberspace* (Basic Books 1999)

Lessig L, *Code: version 2.0* (Basic Books 2006)

- Lessig L, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (Penguin 2004)
- Lessig L, *The Future of Ideas: The Fate of the Commons in a Connected World* (Vintage 2002)
- Lessig L, “The Law of the Horse: What Cyberlaw Might Teach” (1999) 113 *Harvard Law Review* 501
- Levy S, *Hackers: Heroes of the Computer Revolution* (O’Reilly Media, Inc. 2010)
- Levy S, *Crypto: how the code rebels beat the government – saving privacy in the digital age* (Viking 2001)
- Lewis JA, “Government Open Source Policies” <<https://csis.org/publication/government-open-source-policies-0>> accessed 5 February 2016
- Li X, “Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime” (2013) 27 *Harvard Journal of Law & Technology* 301
- Licht AN, “Social Norms and the Law: Why Peoples Obey the Law” (2008) 4 *Review of Law and Economics* 715
- Lindup K, “The Cyberpunk Age” (1994) 13 *Computers & Security* 63
- Lindsay C, “From the Shadows: Users as Designers, Producers, Marketers, Distributors, and Technical Support” in N Oudshoorn and T Pinch (eds), *How Users Matter: The Co-Construction of Users and Technologies* (The MIT Press 2003)
- Litman J, *Digital Copyright* (Prometheus books 2001)
- Lloyd IJ, *Information Technology Law* (Oxford University Press 2008)
- Lloyd, IJ and Simpson M, “Computer Crime” in Chris Reed (ed), *Computer Law* (Blackstone Press 1996)
- Loeber L, “E-Voting in the Netherlands: from General Acceptance to General Doubt in Two Years” in R Krimmer and R Grimm (eds), *Proceedings of 3rd International Conference on Electronic Voting*

2008

Lofgren Z and Wyden R, "Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act" <www.wired.com/opinion/2013/06/aarons-law-is-finally-here/> accessed 2 July 2013

"LOIC" <<http://sourceforge.net/projects/loic/>> accessed on 18 Sept 2014

Longford G, "Pedagogies of Digital Citizenship and the Politics of Code" (2005) 9 *Techne* 68

Lowood H, "Found Technology: Players as Innovators in the Making of Machinima" in T McPherson (ed), *Digital Youth, Innovation, and the Unexpected* (The MIT Press 2008)

Lucchi N, "The supremacy of techno-governance: Privatization of digital content and consumer protection in the globalized information society" (2007) 15 *International Journal of Law and Information Technology* 192

Ludlow P, "Wikileaks and Hactivist Culture" *The Nation* (New York, 4 October 2010)

Luhmann N, *Law as a Social System* (Oxford University Press 2004)

Lunden I, "The Megabreach is back: Hacktivists To Blame for 58 Percent Of Stolen Data In 2011, Says Verizon Study" <techcrunch.com/2012/03/22/the-megabreach-is-back-hacktivists-to-blame-for-58-percent-of-stolen-data-in-2011-says-verizon-study/> accessed 10 February 2013

MacQueen H and others, *Contemporary Intellectual Property: Law and Policy* (Oxford University Press 2011)

Madison MJ, "Legal-ware: Contract and Copyright in the Digital Age" (1998) 67 *Fordham Law Review* 1025

MakerBot, "The MakerBot Way" <www.makerbot.com/blog/2013/06/14/the-makerbot-way/> accessed 21 June 2013

Maker Faire Africa, "This is the Maker Manifesto" <makerfaireafrica.com>

- com/maker-manifesto/› accessed 17 July 2013
- Mancuso V, “5 Hackathon Success Stories” <https://finance.yahoo.com/news/5-hackathon-success-stories-131311777.html> accessed on 15 January 2016
- MapLight, <http://maplight.org/about> accessed by 21 August 2013
- Markoff J, *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry* (Penguin 2005)
- Marsden CT (ed), *Regulating the Global Information Society* (Routledge 2000)
- Maxeiner JR, “Standard-terms Contracting in the Global Electronic Age: European Alternatives” (2003) 28 *Yale Journal of International Law* 109
- Maxigas, “Hacklabs and hackerspaces” (2012) *Journal of Peer Production* Issue #2
- May TC, “The Crypto-Anarchist Manifesto” <http://www.activism.net/cypherpunk/crypto-anarchy.html> accessed 27 May 2014
- McAdams RH and Rasmusen EB, “Norms and the Law” in AM Polinsky and S Shavell (eds), *Handbook of Law and Economics*, Volume 2 (Elsevier 2007)
- McBryde WW, “Remedies for Breach of Contract” (1996) 1 *Edinburgh Law Review* 43
- McCarthy R, “Our Lawyer Explains the Thingiverse Terms of Service” www.makerbot.com/blog/2012/09/26/our-lawyer-explains-the-thingiverse-terms-of-service/ accessed 5 October 2012
- McCullagh D and Homsy M, “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems” (2005) 2005 *Michigan State Law Review* 317
- McLaurin J, “Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks” (2011) 30 *Yale Law & Policy*

Review 211

The Mentor, "The Conscience of a Hacker" Phrack <<http://phrack.org/issues/7/3.html>> accessed 17 July 2013

Michael, George. "The PDP-1" <<http://www.computerhistory.org/pdp-1/>> accessed 11 February 2016

Milan S and Hintz A, "Dynamics of Cyberactivism: Organisations, Action Repertoires, and the Policy Arena" ECPR Conference 2011

Mills E, "Dutch chipmaker sues to silence security researchers" <<http://www.cnet.com/news/dutch-chipmaker-sues-to-silence-security-researchers/>> accessed 11 February 2016

Mills E, "Dutch court allows publication of Mifare security hole research" <<http://www.cnet.com/news/dutch-court-allows-publication-of-mifare-security-hole-research/>> accessed 11 February 2016

Mims III FM, "The Tenth Anniversary of the Altair 8800" Computers & Electronics (January 1985)

"MIT TX-0 Computer 1953", <<http://museum.mit.edu/150/23>> accessed 12 February 2016

Moglen, Eben. "The dotCommunist Manifesto" <http://emoglen.law.columbia.edu/my_pubs/dcm.html> accessed 23 February 2014

Morgan B and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007)

Morison, John. "Modernising Government and the E-Government Revolution: Technologies of Government and Technologies of Democracy" in N Bamforth and P Leyland (eds), *Public Law in a Multi-Layered Constitution* (Hart Publishing 2003)

Moore SF, "Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study" (1973) 7 *Law & Society Review* 719

Morris RT, "A Typology of Norms" (1956) 21 *American Sociological Review* 610

- Munch PA, "Empirical Science and Max Weber's *Verstehen de Soziologie*" (1957) 22 *American Sociological Review* 26
- Murfin M, "Aaron's Law: Bringing Sensibility to the Computer Fraud and Abuse Act" (2014) 38 *Southern Illinois University Law Journal* 469
- Murray A, "Looking Back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important" (2013) 10 *SCRIPTed* 310
- Murray AD, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007)
- Murthy D, "Digital Ethnography: An Examination of the Use of New Technologies for Social Research" (2008) 42 *Sociology* 837
- Naughton J, *A Brief History of the Future: The Origins of the Internet* (Phoenix 1999)
- Nelken D, "The 'Gap Problem' in the Sociology of Law: A Theoretical Review" (1981) 1 *Windsor Yearbook of Access to Justice* 35
- Nelken D, "Law in action or living law? Back to the beginning in sociology of law" (1984) 4 *Legal Studies* 157
- Netherlands Ministry of Security and Justice, National Cyber Security Centre, "Policy of Public Prosecution Service on ethical hackers in line with Responsible Disclosure guidelines" <<https://www.ncsc.nl/english/current-topics/news/policy-of-public-prosecution-service-on-ethical-hackers-in-line-with-responsible-disclosure-guidelines.html>> accessed 21 August 2013
- Netherlands Ministry of Security and Justice, National Cyber Security Centre, "Public-Private Cooperation" <<https://www.ncsc.nl/english/organisation/partners/public-private.html>> accessed 21 August 2013
- The New Hacker's Dictionary, <http://www.outpost9.com/reference/jargon/jargon_toc.html> accessed 12 February 2016
- Nicholson BJ, "The Ghost in the Machine: *MAI Systems Corp. v. Peak Computer, Inc.*, and the Problem of Copying in RAM" (1995) 10

Berkeley Technology Law Journal 147

Nimmer RT, "Breaking Barriers: The Relations Between Contract and Intellectual Property Law" (1998) 13 Berkeley Technology Law Journal 827

Nissenbaum H, "Hackers and the contested ontology of cyberspace" (2004) 6 New Media & Society 195

Nissenbaum H, "How Computer Systems Embody Values" Computer (March 2001)

North, Matthew, Data Mining for the Masses (Global Text Project 2012)

Noveck BS, "Peer to Patent': Collective Intelligence, Open Review, and Patent Reform" (2006) 20 Harvard Journal of Law & Technology 123

Nowotny H, "How Many Policy Rooms are There?: Evidence-Based and Other Kinds of Science Policies" (2007) 32 Science, Technology & Human Values 479

O'Brien K, "Dutch Lawmakers Adopt Net Neutrality Law" <http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=5&pagewanted=all&> accessed 24 June 2015

O'Carroll L, "Scientist banned from revealing codes used to start luxury cars" <<http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars>> accessed 2 March 2015

O'Hear S, "Inside The Billion-Dollar Hacker Club" <<http://techcrunch.com/2014/03/02/w00w00/>> accessed on 10 October 2015

O'Mahony S and Ferraro F, "The Emergence of Governance in an Open Source Community" Technology, Innovation and Institutions Working Paper Series TII-3

Oakes G, "The Verstehen Thesis" (1977) 16 History and Theory 11

Off-the-Record Messaging <<https://otr.cypherpunks.ca/>> accessed on 1 December 2015

- Ohlig J and Weiler L, "Building a Hacker Space" 24th Chaos Communication Congress 2007
- OHM2013, "Call for Participation" <https://ohm2013.org/site/callforparticipation/> accessed 28 November 2012
- OHM2013, "FAQ" <https://ohm2013.org/wiki/FAQ> accessed 23 July 2013
- OHM2013, "Guidelines" <https://ohm2013.org/site/about/578-2/> accessed 23 July 2013
- OHM2013, "Hack" <https://ohm2013.org/site/2013/02/16/hack/> accessed 25 February 2013
- OHM2013, "Make" <https://ohm2013.org/site/2013/02/22/make/> accessed 25 February 2013
- OHM2013, "Observe" <https://ohm2013.org/site/2013/02/08/observe/> accessed 25 February 2013
- OHM2013, "Press release" <https://ohm2013.org/site/press-releases/press-release/> accessed 23 July 2013
- OHM2013, "Program" <https://program.ohm2013.org> accessed 5 August 2013
- OHM2013, "Village:Noisy Square" https://ohm2013.org/wiki/Village:Noisy_Square accessed 24 June 2015
- Olivenbaum JM, "«CTRL» «ALT» «DEL»: Rethinking Federal Computer Crime Legislation" (1997) 27 Seton Hall Law Review 574
- Olson P, We Are Anonymous (Little, Brown and Company 2012)
- Open Cultuur Data, <http://www.opencultuurdata.nl/> accessed 21 August 2013
- Open Data Commons, <http://opendatacommons.org/> accessed 12 August 2013
- Open Data Day 2013, http://wiki.opendataday.org/2013/City_Events accessed 21 August 2013

Open data NEXT, <https://data.overheid.nl/english> accessed 21 August 2013

Open Data Services, <http://www.dati.piemonte.it/> accessed 21 August 2013

“Open Data Sites”, <http://www.data.gov/opendatasites> accessed 12 August 2013

Open Government Initiative, <http://www.whitehouse.gov/open> accessed 12 August 2013

“Open Hardware Constitution”, wiki.openhardware.org/Project:Constitution accessed 12 October 2012

Open Innovatie Festival 2012, <http://www.oif2012.nl/> and <http://www.oif2012.nl/oif058/> accessed 21 August 2013

Open Invention Network, “Defensive Publications” <http://www.defensivepublications.org/> accessed on 9 December 2014

Open Source Hardware Association, “Open Source Hardware (OSHW) Statement of Principles 1.0” <http://www.oshwa.org/definition/> accessed 9 December 2014

Open Source Initiative, “The Open Source Definition” <https://opensource.org/osd> accessed 12 February 2016

Open Technology Fund, “Projects” <https://www.opentechfund.org/projects> accessed 12 February 2016

OpenScience Project, <http://www.openscience.org/blog/> accessed 12 August 2013

“OV-chip” https://ovchip.cs.ru.nl/Main_Page accessed 18 February 2015

Oxblood Ruffin, “Hacktivism” <http://w3.cultdeadcow.com/cms/2000/07/hacktivism.html> accessed 12 February 2016

Opp KD, “Norms” in International Encyclopedia of the Social & Behavioral Sciences (Elsevier Science 2001)

Opsahl K and Samuelson P, “Licensing information in the global

information market: freedom of contract meets public policy”
⟨<http://people.ischool.berkeley.edu/~pam/papers/2bEIPR.pdf>⟩
accessed 15 February 2016

Parker C, “Twenty years of responsive regulation: An appreciation and appraisal” (2013) 7 Regulation & Governance 2

Penfold C, “Nazis, Porn and Politics: Asserting Control Over Internet Content” (2001) Journal of Information, Law and Technology
⟨<http://elj.warwick.ac.uk/jilt/01-2/penfold.html>⟩

Pertierra R, The Anthropology of New Media in the Philippines (Institute of Philippine Culture 2010)

Pettis B, “Fixing Misinformation with Information” ⟨www.makerbot.com/blog/2012/09/20/fixing-misinformation-with-information/⟩ accessed 24 September 2012

Pettis B, “Let’s try that again” ⟨www.makerbot.com/blog/2012/09/24/lets-try-that-again/⟩ accessed 5 October 2012

Pettis B, “Open Source Ethics and Dead End Derivatives” ⟨www.makerbot.com/blog/2010/03/25/open-source-ethics-and-dead-end-derivatives/⟩ accessed 5 October 2012

Pettis B, “Thingiverse updates Terms of Use and License options” ⟨blog.thingiverse.com/2012/02/10/thingiverse-updates-terms-of-use-and-license-options/⟩ accessed 24 September 2012

Pettis B and Stark K, “The Cult of Done Manifesto” ⟨<http://www.brepettis.com/blog/2009/3/3/the-cult-of-done-manifesto.html>⟩ accessed 28 November 2012

Picotti L and Salvadori I, “National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices” (Directorate General of Human Rights and Legal Affairs Council of Europe 2008)

Pinch, Trevor J. and Wiebe E. Bijker, “The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other” (1984) 14 Social

Studies of Science 399

- Platform21, "Repair Manifesto" <www.platform21.nl/download/4375> accessed 28 November 2012
- Pool R, "A History of the Personal Computer" in *Beyond Engineering: How Society Shapes Technology* (Oxford University Press 1977)
- Popper B, "A new breed of startups is helping hackers make millions - legally" <<http://www.theverge.com/2015/3/4/8140919/get-paid-for-hacking-bug-bounty-hackrone-synack>> accessed 22 June 2015
- Posner RA, "Social Norms and the Law: An Economic Approach" (1997) 87 *The American Economic Review* 365
- Press L, "Before the Altair: The History of Personal Computing" (1993) 36 *Communications of the ACM* 27
- Preston-Werner T, "Open Source (Almost) Everything" <tom.preston-werner.com/2011/11/22/open-source-everything.html> accessed 5 October 2012
- Preuschat A, "KPN Admits To Using Deep Packet Inspection" <<http://blogs.wsj.com/tech-europe/2011/05/12/kpn-admits-to-using-deep-packet-inspection>> accessed 24 June 2015
- Principe L, "Renaissance Natural Magic" in *History of Science: Antiquity to 1700* (Teaching Company 2002)
- Prusa, J, "Occupy Thingiverse Test cube" <<http://www.thingiverse.com/thing:30808>> accessed 2 September 2013
- Publicdata.eu, <<http://publicdata.eu/>> accessed 21 August 2013
- Puchner M, "Manifesto = Theatre" (2002) 54 *Theatre Journal* 449
- Raether Jr, R, "Data Security and Ethical Hacking" (2008) 18 *Business Law Today* 55
- Raulerson J, "Cyberpunk Politics: Hacking and Bricolage" in M Learning and B Pretzsch (eds), *Visions of the Human in Science Fiction & Cyberpunk* (Inter-Disciplinary Press 2010)

- Raymond E, “A Brief History of Hackerdom” in *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O’Reilly Media 2001)
- Raymond E, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O’Reilly Media 2001)
- Raymond E, “How to Become a Hacker” <http://www.catb.org/~esr/faqs/hacker-howto.html> accessed 26 January 2016
- Reichman, JH and Franklin JA , “Privately legislated intellectual property rights: Reconciling Freedom of Contract with Public Good Uses of Information” (1999) 147 *University of Pennsylvania Law Review* 875
- Reitman J, “The Rise and Fall of Jeremy Hammond: Enemy of the State” <http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207> accessed 9 December 2012
- “Repair Manifesto” <https://www.ifixit.com/Manifesto> accessed 12 February 2016
- RepRap Project, reprap.org/wiki/Main_Page accessed 30 August 2013
- RepRap, “About” <http://reprap.org/wiki/About> accessed 2 October 2015
- Riseup, <https://help.riseup.net/> accessed 29 July 2015
- Roberts EH and Yates W, “ALTAIR 8000: The most powerful mini-computer project ever presented – can be built for under \$400” *Popular Electronics* (January 1975)
- Rokeach M, *The Nature of Human Values* (The Free Press 1973)
- Rosenbaum R, “Secrets of the Little Blue Box” *Esquire* (October 1971)
- Rosenberg N, “Technological Change in the Machine Tool Industry, 1840-1910” (1963) 23 *The Journal of Economic History* 414

- Ruby JE, “The Origin of Scientific ‘Law’” (1986) 47 *Journal of the History of Ideas* 341
- Rumbles W, “Reflections of Hackers in Legal and Popular Discourse” in W Rumbles (ed), *Cultural Cyborgs* (Inter-Disciplinary Press 2011)
- Samuelson P, “Anticircumvention Rules: Threat to Science” (2001) 293 *Science* 2028
- Samuelson P, “Challenges for the World Intellectual Property Organisation and the Trade-Related aspects of Intellectual Property Rights Council in regulating intellectual property rights in the information age” (1999) 21 *European Intellectual Property Review* 578
- Samuelson P, “Freedom to Tinker” http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605195 accessed 12 February 2016
- Samuelson P, “Hacking Intellectual Property Law” (2008) 51 *Communications of the ACM* 65
- Sather JF, *Understanding the Apple II E* (Quality Software 1985)
- Savage A, “10 Commandments of Making” <http://makezine.com/2014/05/19/adam-savages-10-commandments-of-making/> accessed 3 June 2014
- Schellekens MHM, “Robot.txt: balancing interests of content producers and content users” in R Leenes and E Kosta (eds), *Bridging Distances in Technology and Regulation* (Wolf Legal Publishers 2013)
- Schrock, A, “What Keeps Hacker and Maker Spaces Going?” www.transfabric.org/collectives-in-hacker-and-maker-spaces/ accessed 16 April 2013
- Schultz J and Urban JM, “Protecting Open Innovation: The Defensive Patent License as New Approach to Patent Threats, Transactions Costs, and Tactical Disarmament” (2012) 26 *Harvard Journal of Law & Technology* 1
- Scott J, *A Matter of Record: Documentary Sources in Social Research*

- (Polity Press 1990)
- Sell SK, "TRIPS-plus free trade agreements and access to medicines" (2007) 28 *Liverpool Law Review* 41
- Senfleben M, "Bridging the Differences Between Copyright Legal Traditions - The Emerging EC Fair Use Doctrine" (2009-2010) 57 *Journal Copyright Society of the U.S.A.* 521
- Senfleben M, "Fair Use in The Netherlands - a Renaissance?" (2009) 33 *Tijdschrift voor auteurs, media en informatierecht (AMI)* 1
- Senfleben M, "The International Three-Step Test: A Model Provision for EC Fair Use Legislation" (2010) 1 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 67
- Shmeck, "25 Years of SummerCon" Phrack www.phrack.org/issues.html?issue=68&id=18&mode=txt accessed 24 July 2013
- "A short history of the CCC" in Hackerspaces - The Beginning (2011) <http://archive.org/details/hackerspaces-the-beginning> accessed 2 October 2012
- Slatalla, M and Quittner J, *Masters of Deception: The Gang that Ruled Cyberspace* (HarperCollins 1995)
- Skibell R, "Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act" (2003) 18 *Berkeley Technology Law Journal* 909
- Skibell R, "The Myth of the Computer Hacker" (2002) 5 *Information, Communication & Society* 336
- Socio-Legal Studies Association, "Statement of Principles of Ethical Research Practice" (January 2009)
- Soghoian C, "Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them" (2007) 6 *Northwestern Journal of Technology and Intellectual Property* 46
- Soma JT and others, "Legal Analysis of Electronic Bulletin Board Activities" (1985) 7 *Western New England Law Review* 571

- Soma JT, Winfield G and Friesen L, "Software Interoperability and Reverse Engineering" (1994) 20 Rutgers Computer and Technology Law Journal 189
- Spates JL, "The Sociology of Values" (1983) 9 Annual Review of Sociology 27
- Spurlock J, "A Kit Maker's Manifesto" (<http://makezine.com/magazine/kitguide/maker-manifesto/>) accessed 17 July 2013
- Stallman R, "Initial Announcement" (www.gnu.org/gnu/initial-announcement.html) accessed 7 August 2013
- Stallman R, "The GNU Manifesto" (<https://www.gnu.org/gnu/manifesto.html>) accessed 22 May 2014
- Stallman R, "The GNU Project" (<https://www.gnu.org/gnu/thegnuproject.en.html>) accessed 15 February 2016
- Stallman R, "Why Open Source misses the point of Free Software" (<https://www.gnu.org/philosophy/open-source-misses-the-point.en.html>) accessed 15 February 2016
- Sterling B, The Hacker Crackdown (IndyPublish.com 2002)
- Stratasys, "Stratasys to Acquire MakerBot, Merging Two Global 3D Printing Industry Leaders" (www.businesswire.com/news/home/20130619006431/en/Stratasys-Acquire-Maker-Bot-Merging-Global-3D-Printing) accessed 21 June 2013
- Strauss A and Corbin J, "Grounded Theory Methodology: An Overview" in NK Denzin and Y Lincoln (eds), Handbook of Qualitative Research (Sage Publications 1994)
- Sugru, "The Fixer's Manifesto" (<https://raw.githubusercontent.com/sugru/manifesto/master/manifesto.pdf>) accessed 20 April 2016.
- Sunstein, Cass. "On the Expressive Function of Law" (1996) 144 University of Pennsylvania Law Review 2012
- Swartz A, "Guerilla Open Access Manifesto" (https://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt) accessed 1 February 2013

- Taarifa, <http://taarifa.org/> accessed on 15 January 2016
- Taarifa, <https://taarifa.wordpress.com/> accessed on 15 January 2016
- Tails, <https://tails.boum.org/> accessed on 1 December 2015
- Tactical Technology Collective, “Security in-a-box” <https://tacticaltech.org/projects/security-box> accessed 29 July 2015
- Tamanaha BZ, “Understanding Legal Pluralism: Past to Present, Local to Global” (2008) 30 *Sydney Law Review* 375
- Taylor PA, *Hackers: Crime in the digital sublime* (Routledge 1999)
- Taylor PA, “Editorial: Hacktivism” (2001) 12 *The Semiotic Review of Books* 1
- Taylor PA, “From hackers to hacktivists: speed bumps on the global superhighway” (2005) 7 *New Media & Society* 625
- The Onion Router (Tor), <https://www.torproject.org/> accessed 28 July 2015
- Therborn G, “Back to Norms! On the Scope and Dynamics of Norms and Normative Action” (2002) 50 *Current Sociology* 863
- Thingiverse, <https://www.thingiverse.com/> accessed 12 February 2016
- Thingiverse, “Things tagged with ‘arduino’” <https://www.thingiverse.com/tag:arduino> accessed 12 February 2016
- Thomas D, *Hacker Culture* (University of Minnesota Press 2002)
- Thompson, Clive. “The BitTorrent Effect” <http://www.wired.com/2005/01/bittorrent-2/> accessed 15 February 2016
- Tigoe, “In defense of open source innovation and polite disagreement” www.tigoe.net/blog/category/open-innovation/408/ accessed 5 October 2012
- TNO, “Security Analysis of the Dutch OV-ChipKaart” TNO Report 34643

- Tocchetti S, “DIYbiologists as ‘makers’ of personal biologies: how MAKE Magazine and Maker Faires contribute in constituting biology as a personal technology” (2012) *Journal of Peer Production* Issue #2
- Torrone P, “Life, \$10M in Funding, and Beyond” <http://makezine.com/2011/10/06/makes-exclusive-interview-with-bre-pettis-of-makerbot-life-10m-in-funding-and-beyond/> accessed 12 February 2016
- Torrone P, “The Maker’s Bill of Rights” <http://makezine.com/2006/12/01/the-makers-bill-of-rights/> accessed 27 May 2014
- Torrone P, “Sony’s War on Makers, Hackers, and Innovators” <http://makezine.com/2011/02/24/sonys-war-on-makers-hackers-and-innovators/> accessed 12 February 2016
- Torrone P, “The {Unspoken} Rules of Open Source Hardware” [blog.makezine.com/2012/02/14/soapboxtheunspokenrulesofopen-sourcehardware/](http://blog.makezine.com/2012/02/14/soapbox-the-unspoken-rules-of-open-source-hardware/) accessed 5 October 2012
- Torvalds L and Diamond D, *Just for Fun: The Story of an Accidental Revolutionary* (Thomson TEXERE Publishing 2001)
- Travers M, “Qualitative Interviewing Methods” in Maggie Walter (ed), *Social Research Methods* (Oxford University Press 2013)
- Travers M, *Understanding Law and Society* (Routledge 2010)
- Troxler P, “Libraries of the Peer Production Era” <http://opendesign-now.org/index.php/article/libraries-of-the-peer-production-era-peter-troxler/> accessed 2 April 2013
- Trubek DM and Esser J, “‘Critical Empiricism’ in American Legal Studies: Paradox, Program, or Pandora’s Box” (1989) *14 Law & Social Inquiry* 3
- Turkle S, *Alone Together: Why We Expect More from Technology and Less from Each Other* (Basic books 2012)
- Turkle S, *The Second Self: Computers and the Human Spirit* (The MIT

Press 2005)

Turkle S, “The Subjective Computer: A Study in the Psychology of Personal Computation” (1982) 12 *Social Studies of Science* 173

Tweney D, “DIY Freaks Flock to ‘Hacker Spaces’ Worldwide” www.wired.com/gadgetlab/2009/03/hackerspaces accessed 3 July 2013

“TX-0 Computer” <http://www.computermuseum.li/Testpage/MIT-TX0-Computer.htm> accessed 12 February 2016

Twining W and Miers D, *How to Do Things With Rules: A Primer of Interpretation* (Cambridge University Press 1999)

UK Intellectual Property Office, “Exceptions to copyright: An Overview” (October 2014)

UK Open Access Implementation Group, “The Case for Open Access” <http://open-access.org.uk/case-for-oa/> accessed 15 February 2016

Vance A, “Bre Pettis: 3D Printing’s First Celebrity” www.businessweek.com/articles/2012/05/09/bre-pettis-3d-printings-first-celebrity-2/16 accessed 5 October 2012

van Daalen O, “Netherlands First Country in Europe with Net Neutrality” <https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/> accessed 18 June 2015

van der Meijs S, “Lektoker: iedere dag een privacylek” <http://webwereld.nl/beveiliging/54847-lektoker-iedere-dag-een-privacylek-op-webwereld> accessed 16 June 2015

van der Meijs S, “OM vervolgt Brenno de Winter niet om hack OV-chipkaart” <http://webwereld.nl/overheid/54678-om-vervolgt-brenno-de-winter-niet-om-hack-ov-chipkaart> accessed 16 June 2015

van der Meulen NS and Lodder AR, “Cybersecurity” http://dare.uvu.nl/bitstream/handle/1871/49680/rc2014%20H13%20Van%20der%20Meulen%20Lodder_Cybersecurity_final.pdf?sequence=1 accessed 12 February 2016

- van Eck W, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?” (1985) 4 *Computers & Security* 269
- van Eijk N, “Datalekken: een reality check” <<http://dare.uva.nl/document/2/122176>> accessed 12 February 2016
- van Eijk N, “Net neutrality in practice, the Dutch example” <<http://ssrn.com/abstract=2417933>> accessed 24 June 2015
- van Geelkerken FWJ, “Proposal for the Dutch Computercrime Act III; A critique” <https://www.kau.se/sites/default/files/Dokument/subpage/2011/02/computer_crime_a_critique_pdf_14472.pdf> accessed 12 February 2016
- van Hoboken J, “Relaunch Bits of Freedom!” <<http://www.jorisvan-hoboken.nl/?p=300>> accessed 24 August 2015
- Verizon, “2012 Data Breach Investigations Report”
- Vinje TC, “Compliance with Article 85 in software licensing” (1992) 13 *European Competition Law Review* 165
- von Benda-Beckmann F, “Who’s Afraid of Legal Pluralism?” (2002) 47 *Journal of Legal Pluralism* 37
- von Hippel E, “Democratizing Innovation: The Evolving Phenomenon of User Innovation” (2009) 1 *International Journal of Innovation Science* 29
- Waalboer, Juerd and others, “Open brief aan OM: Hacken” <<http://computervrede.nl/2014-08-26-OpenbaarMinisterie/>> accessed 30 August 2014
- Wall DS, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007)
- Walter, “The Makerbot/Thingiverse move to the Dark Side” <blog.hackerspaces.org/2012/09/23/the-makerbotthingiverse-move-to-the-dark-side/> accessed 24 September 2012
- Maggie Walter (ed), *Social Research Methods* (Oxford University Press 2013)

- Wark M, “A Hacker Manifesto” http://subsol.c3.hu/subsol_2/contributors0/warktext.html accessed 27 May 2014
- “We don’t trust voting computers”, <http://wijvertrouwenstemcomputersniet.nl/English> accessed 12 June 2015
- Weber M, *The Theory of Social and Economic Organization* (The Free Press 1964)
- Webley L, “Qualitative Approaches to Empirical Legal Research” in P Crane and HM Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010)
- Widdison R, “Software Patents Pending” (2000) *The Journal of Information, Law and Technology* <http://elj.warwick.ac.uk/jilt/00-3/widdison.html>
- Williams S, *Free As In Freedom: Richard Stallman’s Crusade for Free Software* (O’Reilly Media 2011)
- Winner, L, *Autonomous Technology: Technics-out-of-control as a Theme in Political Thought* (The MIT Press 1977)
- WIPO International Bureau, “The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)”
- WIPO International Bureau, “The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)”
- WIPO Intellectual Property Handbook (WIPO 2004)
- WIPO Standing Committee on Copyright and Related Rights, “Updated Report on the Questionnaire on Limitation and Exceptions” SCCR/21/7 (2010)
- WIPO Standing Committee on Copyright and Related Rights, “WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment” SCCR/9/7 (2003)
- WIPO Standing Committee on the Law of Patents, “Exclusions from Patentable Subject Matter and Exceptions and Limitations to the Rights” SCP/13/3 (2009)

WIPO Standing Committee on the Law of Patents, "Report on the International Patent System" SCP/12/3 Rev.2, Revised Annex II

Wiseman L, "Beyond the Photocopier: Copyright and Publishing in Australia" (2002) 7 Media & Arts Law Review 299

Wozniak S, "Foreword" in J Sather, Understanding the Apple II E (Quality Software 1985)

Wu T, "Does a Company Like Apple Need a Genius Like Steve Jobs" <http://www.newyorker.com/news/news-desk/does-a-company-like-apple-need-a-genius-like-steve-jobs> accessed 4 March 2013

Wu T, The Master Switch: The Rise and Fall of Information Empires (Vintage 2011)

Wuermeling U, "New Dimensions of Computer-crime - Hacking for the KGB - A Report" (1989-1990) 4 The Computer Law and Security Report 20

Yanoshevsky G, "Three Decades of Writing on Manifesto: The Making of a Genre" (2009) 30 Poetics Today 257

Yiull S, "All Problems of Notation Will Be Solved by the Masses: Free Open Form Performance, Free/Libre Open Source Software, and Distributive Practice" (2004) 10 International Journal of Cultural Policy 64

Yin R, Case Study Research: Design and Methods (Sage Publications 2013)

Ziccardi G, Resistance, Liberation Technology and Human Rights in the Digital Age (Springer Science & Business Media 2012)

Zijlstra T, "The State of Open Data in Europe - Achievements and Challenges" <http://www.zijlstra.org/blog/2013/02/the-state-of-open-data-in-europe-achievements-and-challenges/> accessed 21 August 2013

Zittrain J, The Future of the Internet - And How to Stop It (Yale University Press 2008)

Zuckerberg M, "The Hacker Way" www.wired.com/business

ness/2012/02/zuck-letter/› accessed 19 August 2013

Zuiderwijk A and others, “Socio-technical Impediments of Open Data” (2012) 10 *Electronic Journal of e-Government* 156

Zumbansen P, “Transnational Legal Pluralism” *Comparative Research in Law & Political Economy Research Paper* 01/2010

Treaties, statutes and legislation

Agreement on Trade-Related Aspects of Intellectual Property Rights

Australian Copyright Amended Act 2006

Berne Convention for the Protection of Literary and Artistic Works

Brazilian Criminal Code

Commission Decision of 12 December 2011 on the reuse of Commission documents (2011/833/EU)

Convention on Cybercrime

Convention on the Grant of European Patents (European Patent Convention)

Council Directive of 1 May 1991 on the legal protection of computer programs (as amended and codified by Directive 2009/24/EC)

Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [2005] OJ L069

Directive 96/9/EC on the legal protection of databases

Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society

Directive 2003/98/EC of the European Parliament and the Council on the re-use of public sector information

Directive 2009/24/EC on the legal protection of computer programs

Directive 2013/37/EU of the European Parliament and of the Council amending Directive 2003/98/EC on the re-use of public sector information

Dutch Copyright Act

Dutch Criminal Code

Dutch Patent Act

European Commission, “Proposal for a Directive on attacks against information systems” COM(2010) 517

European Commission, “Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA” COM(2010) 517

European Commission, “Communication on Open data: An engine for innovation, growth and transparent governance”

European Commission, “Guidelines on recommended standard licences, datasets and charging for the reuse of documents” (2014/C 240/01)

European Commission, “Proposal for a Directive on Amending Directive 2003/98/EC on re-use of public sector information”

European Commission, “Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA”, COM(2010) 517

Explanatory Report to the Convention on Cybercrime

Netherlands Ministry of Security and Justice, National Cyber Security Centre, “Policy for arriving at a practice for Responsible Disclosure”

Paris Convention for the Protection of Industrial Property

Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems (1990)

Report on application of Directive 2001/29/EC SEC(2007) 1554

Slovakian Criminal Code

Treaty on Intellectual Property in Respect of Integrated Circuits

US Copyright Act 1976

US Computer Fraud and Abuse Act

US Digital Millennium Copyright Act

WIPO, Agreed Statements concerning the WIPO Copyright Treaty
1996

WIPO Copyright Treaty

WIPO Performances and Phonograms Treaty

Cases

Authors Guild v. Hathitrust 755 F.3d 87 (2014)

British Academy of Songwriters, Composers and Authors Musicians' Union v Secretary of State for Business, Innovation and Skills [2015] EWHC 2041 (Admin) (17 July 2015)

Canada - Patent Protection of Pharmaceutical Products, WT/DS114/R (17 March 2000)

Case C-406/10 SAS Institute Inc. v World Programming Ltd [2012]

Chamberlain Group v Skylink Technologies 381 F. 3d 1178 (2004)

Diamond v. Diehr 450 U.S. 175 (1981)

Field v. Google 412 F.Supp.2d 1106 (2006)

Folsom v Marsh (1841)

Krause v Titleserv, Inc., 402 F.3d 119 (2005)

Lexmark v. Static Control Components, 387 F.3d 522 (2004)

MDY Industries, LLC. v. Blizzard Ent., Inc., 616 F. Supp. 2d 958 (2009).

MDY Industries v Blizzard Entertainment, 629 F. 3d 928 (2010)

NXP Semiconductors vs Radboud Universiteit Nijmegen, Arnhem Court Case Number 171900 (18 July 2008)

Recording Industry Association of America v. Diamond Multimedia Systems 180 F.3d 1072 (1999)

SCO Group v. IBM WL 318784 (2005)

Sony v. Universal 464 U.S. 417 (1984)

Storage Technology v. Custom Hardware Engineering, 421 F.3d 1307 (2005)

TracFone Wireless, Inc. v. Dixon, 475 F. Supp. 2d 1236 (2007)

United States v Gilberto Valle, No. 14□2710□cr and No. 14□4396□cr (3 December 2015)

Universal City Studios v Reimerdes 111 F.Supp.2d 294 (2000)

Universal City Studios v Corley, 273 F.3d 429 (2001)

The relationship between hacking and the law has always been complex and conflict ridden. Hackers have been the perennial subjects and targets of law and criminal prosecution, yet they are also known to have problems with law and public authorities. This book examines the relations and interactions between hacking and the law with a view to understanding how hackers influence and are influenced by technology laws and policies. In an increasingly digital and connected world where hackers play a significant role in determining the structures, configurations and operations of the networked information society, an interdisciplinary study of hacking that combines the fields of technology law, socio-legal studies, and science and technology studies is essential in order to properly comprehend and address the socio-technical changes and consequent legal challenges that society faces. This book principally aims to describe and analyze the legal and normative impact of hackers and to propose improved approaches to the regulation and governance of hacking as well as technology as a whole.

Michael Anthony C. Dizon is an information and communications technology lawyer and researcher. His work mainly involves the socio-legal study of technology, creativity and innovation. He has conducted research at universities and academic institutes in the Netherlands, the United Kingdom and the Philippines. He has also practiced as a lawyer at various law firms and companies.