



# Encryption and the manifold meanings of security

Michael Dizon, PhD . Te Piringa – Faculty of Law, University of Waikato



# Overview

- 1 Encryption and international and national security
- 2 Different meanings of security vis-à-vis encryption
  - Technical
  - Legal and social
- 3 Application to major encryption and security issues
- 4 Conclusion



# 1.1 Encryption and security

- Neither novel nor new
- Used by rulers, governments and other public actors for military and intelligence purposes for millennia
- Utilised by individuals and private actors to keep information private and communications and correspondences secret



# 1.2 Encryption affects security

- Application in computer and other information technologies and use across online networks and digital media
- New technical, legal and social problems and issues
- Debate over encryption, security and privacy
- Make explicit the varied meanings of security vis-à-vis encryption
- Talking about different things





# 1.3 Definition of encryption

- Encryption is a technology that transforms information or data into ciphers or code for purposes of ensuring the confidentiality, integrity and authenticity of such data or a related system



# 2 Meanings of security

## Technical

Information security

- Confidentiality
- Integrity
- Authenticity

Secrecy and  
inviolability of keys

Level of security

- Unconditional security
- Computational or provable security

## Legal and social

National security

- Public order and safety
- Law enforcement and criminal investigations and prosecutions

Privacy

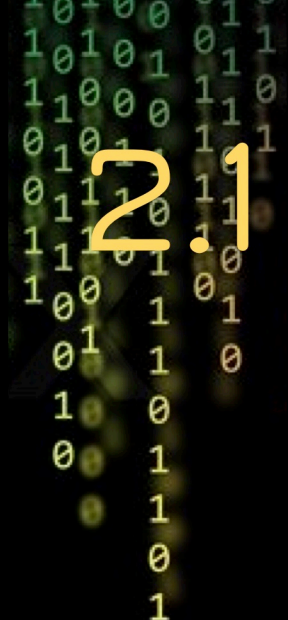
- Informational privacy
- Communicational privacy, intellectual privacy, and associational privacy

Right against unreasonable search and seizure

- Security of physical and intangible things
- Secrecy of correspondence

Right against self-incrimination

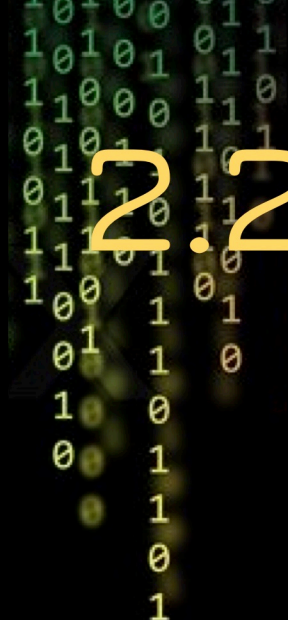
Data protection



## 2.1

# Information security

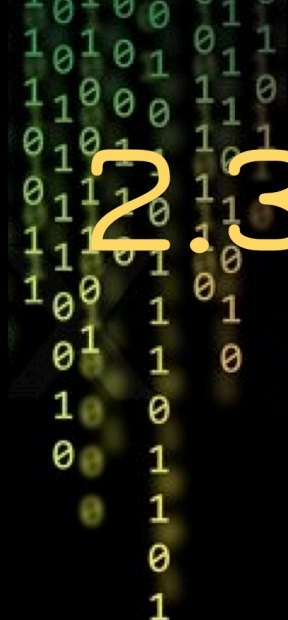
- Protect and preserve the confidentiality, integrity and authenticity of computer data and systems
  - Confidentiality – data kept secret from unauthorised persons
  - Integrity – data unaltered by unauthorised parties
  - Authenticity – identification of the sender and confirmation that the data was actually sent by the sender (includes non-repudiation)
- Encryption is essential for any or all information security objectives



## 2.2

# Secrecy and inviolability of keys

- Primacy of keys
- Keep keys secret and safe from unauthorised parties
- Otherwise insecure

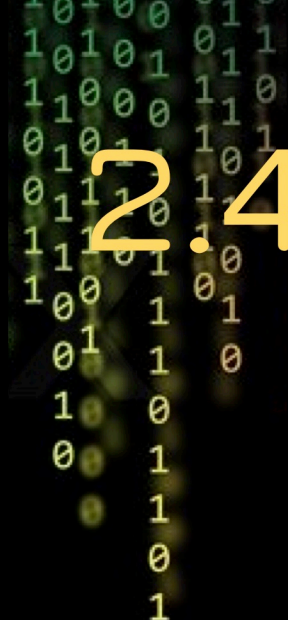


## 2.3

# Level of security

- Unconditional security – perfect secrecy
- Provable security – impracticability and infeasibility of attacks
- Insecure

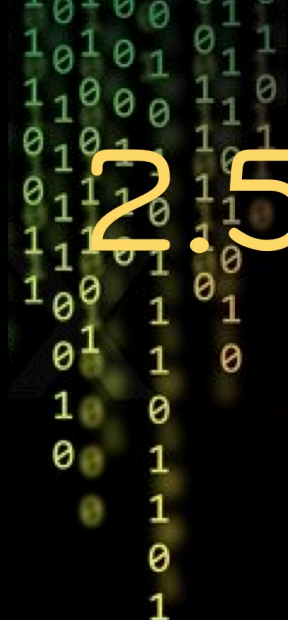




## 2.4

# National security

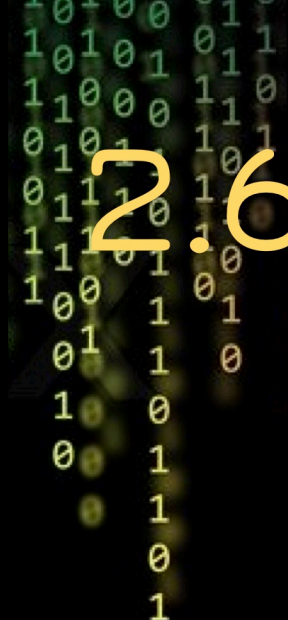
- “The safety of a nation against threats such as terrorism, war, or espionage”
- Nation-state
- Public order and safety
- Law enforcement and criminal investigations and prosecutions



## 2.5

# Privacy

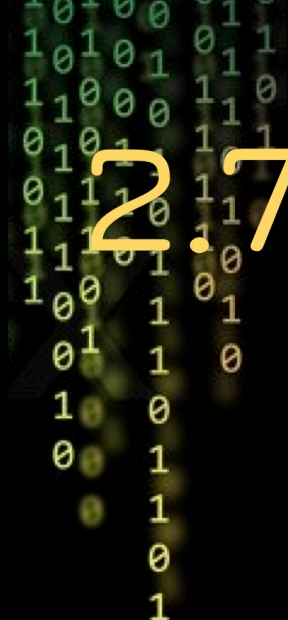
- Right to be left alone
- 9 basic types: bodily, spatial, communicational, proprietary, intellectual, decisional, associational, behavioural, and informational (Koops and others)
- Most relevant to encryption
  - Informational privacy
  - Communicational privacy, intellectual privacy, and associational privacy



## 2.6

# Right against unreasonable search and seizure

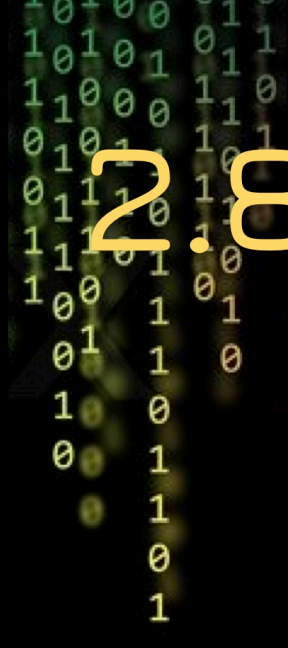
- “Everyone has the right to be *secure* against unreasonable search or seizure, whether of the *person, property, or correspondence* or otherwise”
- Security of *physical* beings, things and locations and *intangible* things and information
- Includes the right to secrecy of correspondence or confidentiality of communications



## 2.7

# Right against self-incrimination

- “The right not to be compelled to be a witness or to confess guilt”
- Minimum standards of criminal procedure
- Defence against forced password disclosure for persons criminally charged or accused
- Protection against a forced confession



## 2.8

# Data protection

- Connected to privacy and information security
- Protection of personal data, specifically with respect to its processing
- Personal data is “any information relating to an identified or identifiable natural person” (GDPR)
- Data protection principle of integrity and confidentiality



# 3.1

## Application: Backdoors

### Technical

#### Information security

- Confidentiality
- Integrity
- Authenticity

Secrecy and inviolability of keys

#### Level of security

- Unconditional security
- Computational or provable security

### Legal and social

#### National security

- Public order and safety
- Law enforcement and criminal investigations and prosecutions

#### Privacy


- Informational privacy
- Communicational privacy, intellectual privacy, and associational privacy

#### Right against unreasonable search and seizure

- Security of physical and intangible things
- Secrecy of correspondence

#### Right against self-incrimination

#### Data protection



32

# Forced disclosure of passwords

## Technical

Information security

- Confidentiality
- Integrity
- Authenticity

## Secrecy and inviolability of keys

Level of security

- Unconditional security
- Computational or provable security

## Legal and social

National security

- Public order and safety
- Law enforcement and criminal investigations and prosecutions

Privacy

- Informational privacy
- Communicational privacy, intellectual privacy, and associational privacy

Right against unreasonable search and seizure

- Security of physical and intangible things
- Secrecy of correspondence

## Right against self-incrimination

Data protection



33

# Lawful access and interception

## Technical

Information security

- **Confidentiality**
- Integrity
- Authenticity

Secrecy and inviolability of keys

Level of security

- Unconditional security
- Computational or provable security

## Legal and social

National security

- Public order and safety
- **Law enforcement and criminal investigations and prosecutions**

Privacy

- Informational privacy
- Communicational privacy, intellectual privacy, and associational privacy

Right against unreasonable search and seizure

- Security of physical and intangible things
- **Secrecy of correspondence**

Right against self-incrimination

Data protection

# 34

## National security and privacy

### Technical

Information security

- **Confidentiality**
- Integrity
- **Authenticity**

Secrecy and inviolability of keys

Level of security

- Unconditional security
- Computational or provable security

### Legal and social

National security

- **Public order and safety**
- **Law enforcement and criminal investigations and prosecutions**

Privacy

- Informational privacy
- **Communicational privacy**, intellectual privacy, and **associational privacy**

Right against unreasonable search and seizure

- Security of physical and intangible things
- Secrecy of correspondence

Right against self-incrimination

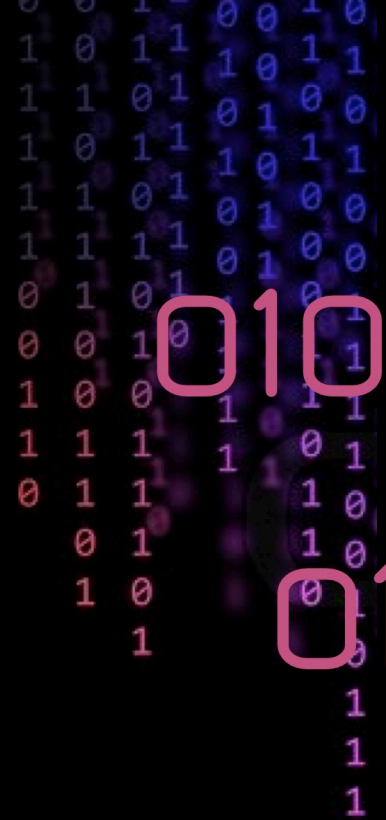
Data protection



# 4 Conclusion

- Security has multiple meanings
- Understand which specific meanings apply
- Stronger possibility of resolving problems concerning encryption
- What people are actually talking about





01010001

and

01000001

Questions ?