Matters of trust, privacy and security:

An examination of the technical, legal and social principles and values of encryption

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

Overview

1. Technical principles and rules
2. Legal rules
3. Fundamental principles and values
4. Conclusions and recommendations
5. Questions and comments

1 Technical principles and rules

Principles and rules

- Information security
  - Confidentiality, integrity and authenticity
- Primacy of keys
  - Secrecy and inviolability
- Openness
  - Publicly accessible, transparent and auditable

Principles and rules

- Adversarial nature
- Resistance to attacks
- Appropriate level of security
  - Unconditional security
  - Computational or provable security

2 Legal rules

Laws of encryption

- Export control rules
- Cybercrime laws
- Law enforcement and criminal procedure (including search and surveillance laws)
- Human rights laws

Export control and cybercrime

- Export control rules – prior approval before export of dual-use technology
- Cybercrime laws – Making, selling, distributing or possessing software for committing crime

Law enforcement – search and seizure

- Search and seize encrypted data (data at rest), devices and systems
- Power to request reasonable and necessary assistance
- Power to require the disclosure of access information (including passwords and encryption keys)
- Applies to suspects and third party developers
- Penalty of imprisonment for refusal to comply

Law enforcement – surveillance

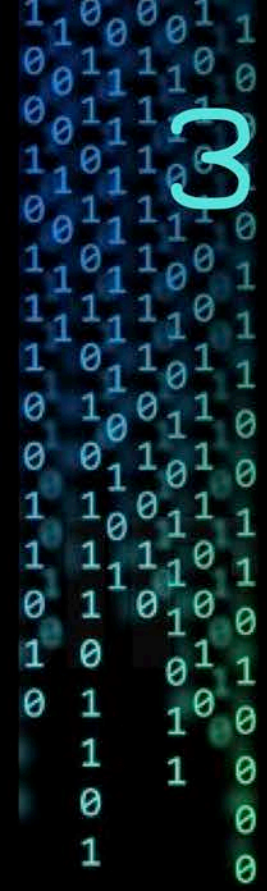
- Power to intercept and collect encrypted communications (data in motion)
- Networks operators required to permit lawful access to their networks
- Network operators and service providers duty to give reasonable assistance to intercept and collect

Law enforcement – production order

- Produce existing encrypted documents and data
- Traffic data, subscriber data and other metadata

Human rights

- Right against unreasonable search and seizure
  - Standard of reasonableness
- Right against self-incrimination
  - Only applies when access information *itself* incriminating?
  - Any information that would tend to incriminate a person



3 Fundamental principles and values of encryption

Ten fundamental principles and values

- Data protection
- Information security
- Law enforcement and lawful access
- National security and public safety
- Privacy
- Right against self-incrimination
- Right against unreasonable search and seizure
- Right to property
- Secrecy of correspondence
- Trust

Categories

Human rights and freedoms	Law enforcement and public order
Data protection	Law enforcement and lawful access
Privacy	National security and public safety
Right against self-incrimination	
Right against unreasonable search and seizure	
Right to property	
Secrecy of correspondence	
Information security	
Trust	

Ranking of principles and values

- Focus group interviews with 3 groups of stakeholders: general public, business and government

- Ranking exercise

Ranking across all stakeholders

Top tier

1. Privacy
2. Data protection
3. Information security
4. Trust
5. National security and public safety
6. Right to property

Second tier

7. Secrecy of correspondence
8. Law enforcement and lawful access
9. Right against unreasonable search and seizure
10. Right against self-incrimination

Ranking compared

	Overall	General public	Business	Government
	Top tier			
1	Privacy	Privacy	Information security	Privacy
2	Data protection	Data protection	Data protection	National security & public safety
3	Information security	Information security	National security & public safety	Trust
4	Trust	Trust	Privacy	Data protection
5	National security & public safety	Right to property	Right to property	Right to property
6	Right to property	Secrecy of correspondence	Trust + Secrecy of correspondence	Right vs. unreasonable search & seizure
	Second tier			
7	Secrecy of correspondence	National security & public safety		Law enforcement & lawful access
8	Law enforcement & lawful access	Law enforcement & lawful access	Law enforcement & lawful access	Information security
9	Right vs. unreasonable search & seizure	Right vs. unreasonable search & seizure	Right vs. self-incrimination	Secrecy of correspondence
10	Right vs. self-incrimination	Right vs. self-incrimination	Right vs. unreasonable search & seizure	Right vs. self-incrimination

Relationship between principles and values

- Focus group participants
- Organise and visualise the relations between the principles and values

Business

National security & public safety	Information security
Right vs. unreasonable search & seizure	Trust
Law enforcement & lawful access	Privacy
Right vs. self-incrimination	Data protection
Right to property	Secrecy of correspondence

General public

Right to property

Information security

Secrecy of correspondence

Data protection

Privacy

Trust

Law enforcement & lawful access

National security & public safety

Right vs. self-incrimination

Right vs. unreasonable search & seizure

Government

	Trust	
Law enforcement & lawful access	National security & public safety	Right to property
Right vs. unreasonable search & seizure	Right vs. self-incrimination	Secrecy of correspondence
Data protection	Privacy	Information security

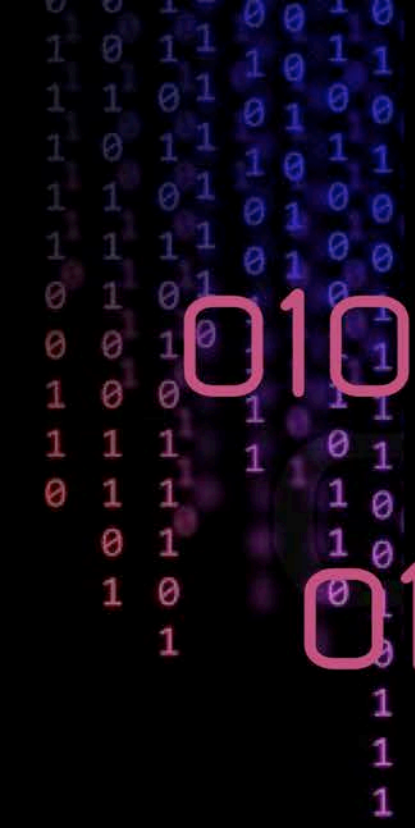
4 Conclusions and recommendations

Policy recommendations

- Integral to information security
- Necessary to protect privacy and data protection
- Involves law enforcement and public order concerns

Policy recommendations

- The right against unreasonable search and seizure and the right against self-incrimination are critical
- Requires balancing and reconciling competing interests
- Fundamentally relies on trust



01010001

and

01000001

Questions ?