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

<table>
<thead>
<tr>
<th>Human rights and freedoms</th>
<th>Law enforcement and public order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection</td>
<td>Law enforcement and lawful access</td>
</tr>
<tr>
<td>Privacy</td>
<td>National security and public safety</td>
</tr>
<tr>
<td>Right against self-incrimination</td>
<td></td>
</tr>
<tr>
<td>Right against unreasonable search and seizure</td>
<td></td>
</tr>
<tr>
<td>Right to property</td>
<td></td>
</tr>
<tr>
<td>Secrecy of correspondence</td>
<td></td>
</tr>
<tr>
<td>Information security</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Overall</th>
<th>General public</th>
<th>Business</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top tier</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Privacy</td>
<td>Privacy</td>
<td>Information security</td>
<td>Privacy</td>
</tr>
<tr>
<td>2 Data protection</td>
<td>Data protection</td>
<td>Data protection</td>
<td>National security &amp; public safety</td>
</tr>
<tr>
<td>3 Information security</td>
<td>Information security</td>
<td>National security &amp; public safety</td>
<td>Trust</td>
</tr>
<tr>
<td>4 Trust</td>
<td>Trust</td>
<td>Privacy</td>
<td>Data protection</td>
</tr>
<tr>
<td>5 National security &amp; public safety</td>
<td>Right to property</td>
<td>Right to property</td>
<td>Right to property</td>
</tr>
<tr>
<td>6 Right to property</td>
<td>Secrecy of correspondence</td>
<td>Trust + Secrecy of correspondence</td>
<td>Right vs. unreasonable search &amp; seizure</td>
</tr>
<tr>
<td><strong>Second tier</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Secrecy of correspondence</td>
<td>National security &amp; public safety</td>
<td>Law enforcement &amp; lawful access</td>
<td></td>
</tr>
<tr>
<td>8 Law enforcement &amp; lawful access</td>
<td>Law enforcement &amp; lawful access</td>
<td>Law enforcement &amp; lawful access</td>
<td>Information security</td>
</tr>
<tr>
<td>9 Right vs. unreasonable search &amp; seizure</td>
<td>Right vs. unreasonable search &amp; seizure</td>
<td>Right vs. self-incrimination</td>
<td>Secrecy of correspondence</td>
</tr>
<tr>
<td>10 Right vs. self-incrimination</td>
<td>Right vs. self-incrimination</td>
<td>Right vs. unreasonable search &amp; seizure</td>
<td>Right vs. self-incrimination</td>
</tr>
</tbody>
</table>
Relationship between principles and values

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

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

- National security & public safety
  - Right vs. self-incrimination
  - Privacy

- Right to property
  - Secrecy of correspondence
  - 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
010000001

Questions