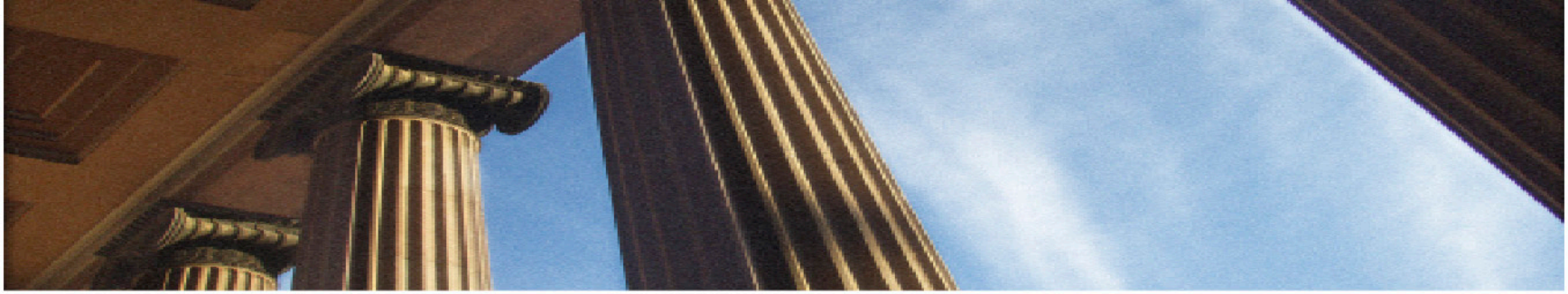

UiO : Department of Private Law
University of Oslo

Assistance and Access Act (Australia): the Latest Government Attempt to Resist "Going Dark"

Peter Davis, NRCCL
p.a.e.davis@jus.uio.no

Barr Revives Encryption Debate, Calling on Tech Firms to Allow for Law Enforcement

The attorney general, reopening the conversation on security vs. privacy, said that encryption and other measures effectively turned devices into "law-free zones."

Source: NY Times, 23 July 2019

How/Why to Regulate Cryptography?

- **Promote** the use of strong cryptography: ensure that entities are utilising appropriate security measures to protect the CIA of NIS
- **Discourage or restrict**, through regulatory measures, use of (strong) cryptography so that 'bad guys' cannot hide their communications
- **Restrict the export of cryptographic algorithms:** So other countries cannot use your country's strong cryptographic algorithms

UiO : Department of Private Law
University of Oslo

THE CRYPTO WARS & 'GOING DARK' – THE LAW AS UNDERMINING ENCRYPTION

‘First’ Crypto Wars

- A series of actions primarily through regulation by the US administration (and others), in the early 1990s, that attempted to limit or slow the public’s (and foreign nations’) access to crypto that US (and its allies’) intelligence and law enforcement would be unable to decrypt, including:
  - Export controls on cryptography as munitions or dual-use items (CoCom: WWII-1994; Wassenaar Arrangement: 1996-present);
  - The ‘Clipper Chip’ (1993-1996).
- Two threats:
  - That the US would no longer be ahead of the cryptography ‘arms race’; and
  - With the rise of the internet, the use of cryptography would be come ubiquitous amongst the public, and not just used by the government or military

Crypto-Wars 2.0 – Going Dark / Going Spotty

- 2011: then-FBI General Counsel refers to ‘going dark’
- 2013: Edward Snowden revelations
  - PRISM programme (2007-?)
    - Participants: Microsoft, Google, Facebook, Apple
    - September 2014: Apple and Google announce encryption by default in next iOS / Android versions
    - November 2014: WhatsApp switches to end-to-end encryption
  - Bullrun programme (2000-?)
- 2016: Apple vs FBI (San Bernadino case)
- Recent legislative initiatives
  - *Investigatory Powers Act* (2016) (UK)
  - *Assistance and Access Act* (Dec 2018) (Australia)

‘Rights’ and Crypto Issues

- Freedom of Expression/Speech
  - 1st Amendment US Const., Art 10 ECHR, Art 11 EU Charter, Art 19 UDHR & ICCPR
  - *Bernstein v United States* – (crypto) code is speech
  - Apple vs FBI – ‘compelled speech’
- Right to privacy / data protection
  - 4th Amendment US Const., Art 8 ECHR, US Art 11 UDHR, Art 17 ICCPR
- Privilege against self incrimination / right to remain silent
  - Laws requiring decryption by suspect – text or biometric password
  - 5th Amendment US Const., inherent in e.g. right to fair trial Art 6 ECHR
- Rights against unreasonable searches and seizures
  - 4th Amendment US Const. – easier to use
- Human right to use strong encryption? Right to cybersecurity?
- Crypto as ‘arms’ -> right to bear arms (2nd Amendment)?

Possible Legal Solutions to Going Dark (Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' problem*)

1. Criminalise supply, possession or use of (certain) cryptographic technologies (in certain situations)
   - E.g. Russia's ban of Telegram
   - Can't distinguish between legitimate and illegitimate uses
   - Availability of open-source encryption on the internet
   - Strong crypto already ubiquitous (horse has bolted)
   - Impact on economy (First Crypto wars)
   - Freedom of speech (*Bernstein v US*)
2. Compulsory disclosure of keys (when suspect of a crime or target of investigation)
   - Conflict to privilege against self-incrimination / right to remain silent
   - Works for *ex post* (law enforcement) but not *ex ante* (intelligence gathering)
   - "I can't remember"

Possible Legal Solutions to Going Dark (Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' problem*)

3. Service provider assistance, e.g. 'Snoopers Charter' (UK); *Assistance and Access Act 2018* (Aus)
   - End-to-end encryption and certain types of disk encryption (e.g. iOS 9 onwards) -> no assistance possible?
   - Human rights issues e.g. right to privacy
4. Mandatory backdoors / key escrow / exceptional access
   - E.g. Clipper Chip (1990s); GCHQ Ghost Protocol (Nov 2018); Ray Ozzie 'Clear' (Jan 2017)
   - Undermining of cybersecurity
   - Open-source software
   - Human rights
   - Tension with other cybersecurity law e.g. Art 25 GDPR

Possible Legal Solutions to Going Dark (Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' problem*)

5. Infiltration of (criminal/terrorist) networks
   - Difficult and expensive; entrapment
6. Break the protection (e.g. brute-force attacks on cryptography or exploitation of software weaknesses/ zero days)
   - Cryptography is strong and breaking it is expensive (Bullrun 2011-13 cost $800m USD according to Snowden)
   - Legal issues (e.g. right against unlawful search and seizure)
   - Cybersecurity issues relating to zero days (e.g. NSA hack and WannaCry) -> vulnerabilities equities process?
   - Purchase of vulnerabilities by private entities (NSO Group, Cellebrite, Azimuth) -> similar legal issues to gov-created vulns (i.e. is evidence lawfully obtained?). Also moral issues?

Possible Legal Solutions to Going Dark (Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' problem*)

7. Focus on metadata
   - Not as useful as content data
   - Human/fundamental rights issues relating to mandatory storage of metadata by telcos (CJEU in *Digital Rights Ireland* invalidating *Data Retention Directive* 2006/24/EC)

#waronmaths

- Malcolm Turnbull, Prime Minister of Australia
  - "The privacy of a terrorist can never be more important than public safety – never." June 2017
  - "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." – July 2017
- Why Australia?
  - Only Western democracy with no* enforceable human rights protections at the federal (national) level
  - Member of 5 eyes - forum shopping?

Telecommunications & Other Legislation Amendment (Assistance & Access) Act 2018 (Cth)

- Amends every federal-level surveillance legislation in Australia
- Establishes new obligations for communications providers
- Extremely wide scope: any website providers or designers of hardware/software (likely to be) available in Australia
  - E.g. mobile/internet providers, handset manufacturers, owners or suppliers of telecommunication infrastructure
- Applies extraterritorially (though unclear how in practice)

Assistance and Access Act

Schedule 1 – amends *inter alia* the *Telecommunications Act* (>1000 pages)

- Technical Assistance Request (**TAR**)
- Technical Assistance Notice (**TAN**)
- Technical Capability Notice (**TCN**)
- All 3 can be issued in relation to:
  - Serious criminal offences (max penalty >3 years)
  - Assisting the enforcement of criminal laws in a foreign country (including w/possible death penalty); or
  - Safeguarding national security (not defined).
- TARs only can be issued in relation to the above, but also *inter alia* Australia's economic wellbeing, foreign relations

Technical Assistance Requests (TARs)

- Agencies can request a provider to do a range of ‘acts or things on a **voluntary** basis’ to assist LEA/intelligence
- No penalties for non-compliance; but penalties for unauthorised disclosure
- No judicial oversight

Assistance and Access Act

- Technical Assistance Notice (**TAN**)
  - Similar to UK *Investigatory Powers Act* 'technical capability notice' (section 253)
  - Agencies can compel a provider to do a range of 'acts or things' to give assistance that it is already capable of
  - Must be reasonable, proportionate, practicable and technically feasible
    - E.g. agencies can ask providers to decrypt communications where they have the ability to do so (i.e. not true end-to-end)
  - Requires underlying warrant but not fresh judicial approval
  - Civil penalties up to $10m AUD for non-cooperation
  - Cannot require a provider to implement a *systemic weakness* or *systemic vulnerability*

Assistance and Access Act

- Technical Capability Notice (**TCN**)
  - Not to be confused with UK *Investigatory Powers Act* 'technical capability notice'
  - Agencies can issue a TCN requiring a provider to build or implement a new technical capability allowing it to assist agencies
  - Must be reasonable and proportionate
  - Civil penalties up to $10m AUD for companies for non-cooperation
  - Cannot require a provider to implement a *systemic weakness* or *systemic vulnerability*

Article 317ZG

- Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.
  - A request/notice must not have the effect of
    - Requiring implementation or building of systemic weakness/vulnerability
    - Preventing the rectification of systemic weakness/vuln

Article 317ZG / ‘systemic weakness’

- **systemic weakness/vulnerability** means a weakness/vulnerability that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person.
- “includes a reference to implement or build a new decryption capability in relation to a form of electronic protection.”
  - Electronic protection ‘includes authentication, encryption’
- “includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.”
- Includes “an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.”

Systemic Weakness / Vulnerability

- Difference between weakness and vulnerability?
- What is a ‘whole class of technology’?
  - Class is not defined by the Act
  - Broad definition: class = phone / computer / tablet
  - Narrow definition: class = specific device and software (e.g. iPhone X running iOS 12.4)
- Is any ‘weakness’ a ‘systemic weakness’?
  - Does the mere existence of a weakness/vuln ‘create a material risk that otherwise secure info can be accessed by an unauthorised third party’?

Other concerns

- Australian companies are less secure than non-Australian companies?
  - Theoretically, international companies are subject to the same laws if they are a ‘designated communications provider’ that conducts ‘eligible activities’ (s 317C)
  - But more difficult to apply to intl companies in practice
- An employee can be forced to conduct corporate espionage by the Australian government?
  - False – notice/request must be sent to registered office of company (or agent/business address) (s 317ZL)
  - True that harsh penalties for unauthorised disclosure, including by employees (max 5 years imprisonment) (s 317ZF)
- Forum shopping?

Significance for Going Dark Debate

- The UK and Australian approaches signal a shift from the ‘backdoors’ / key escrow debate and towards a ‘side doors’ / lawful hacking / industry assistance approach
  - i.e. acknowledging that putting vulnerabilities in crypto is a flawed idea
- But AG Barr’s comments suggest Trump admin might return to old habits
  - Notably, first time a US official has accepted that any measure would reduce overall level of cybersecurity