Law

LAW

Internet-specific laws prior to 2000 were generally not needed because most illegal activities on the Internet were covered by non-internet equivalents:

- fraud, harassment, theft, stalking, censorship, breaking and enteringThird level

Identity theft is an emerging problem, so new laws are being developed around the world.

- In Australia, the Internet is predominately regulated by laws relating to media and telecommunications.
- Australian laws specific to the Internet include censorship

Law

Internet-specific laws prior to 2000 were generally not needed because most illegal activities on the Internet were covered by non-internet equivalents:

- fraud, harassment, theft, stalking, censorship, breaking and enteringThird level

Identity theft is an emerging problem, so new laws are being developed around the world.

- In Australia, the Internet is predominately regulated by laws relating to media and telecommunications.
- Australian laws specific to the Internet include censorship

MORE LAW

- Cyber-terrorism, (evil) hacking, DDOS and extortion are increasing.
- Internet-based espionage is flourishing.
- Technology for automated MITM of SSL is available to governments to spy on their citizens. http://www.packetforensics.com/products.safe
- Technology for detecting key-words (Carnivore) is spreading around the world
- USA, China, UAE, Saudi-Arabia, Swinburne?

AUSTRALIAN LAWS

Copyright Amendment Act (2000)

1. Fair Dealing exceptions (e.g. photocopying) for study/research/review
2. ISPs classified as common carriers – not responsible for copyright infringements (e.g. Torrents). Recently tested and confirmed (iiNet)
3. OK to re-transmit content
4. Backing up software allowed
5. Copyright extended to Internet, digital copies

AUSTRALIAN LAWS

Cybercrime Act (2001)

1. Terms updated to include USB disks, network storage, wifi.
2. Other terms updated
   - unauthorized access (breaking in)
   - modification
   - impairment (DOS)
3. Accidentally breaching security is not always an offence.
4. ISPs must report suspicious activities to AFP

BUT…

Cybercrime Act (2001)

1. ASIS and DSD granted immunity from prosecution for doing their job
2. Allowed to compel people to help them
3. Penetration testing now illegal
   - Aust. sites less hardened to attack
   - Softer targets for crackers
   - Still OK if you get written and scoped permission from the owner

CONTINUED

Spam Act (2003)

1. Spam must not be sent.
   - Covers e-mail, SMS, MMS, IM
   - Fax, Web pop-ups, telemarketing not prohibited.
2. Commercial mail must reveal who authorised it
3. E-mail harvesting software is illegal
4. Mailing lists created by (3) must not be used
5. Opt-in required.
6. Unsubscribe link required

CONTINUED

Surveillance Devices Act (2004)

- Police allowed to use spyware / trojans to gather evidence.
- Keyloggers
- RATs

http://www.computerworld.com/s/article/9249352

CONTINUED

Copyright law amendments (2006)

- Time-shifting now legal – record and play once
  - Lending recordings prohibited
- Backups now permitted
- Transfers to tape/disk/iPod now permitted

CYBERCRIME LEGISLATION AMENDMENT BILL 2011

In force 1 March 2013

LE agencies can request preservation of communications that carriers store, such as SMS messages, and that can be accessed only under a warrant

- Greater co-operation with overseas LE in the investigation of cybercrime.
- Makes our laws compliant with Council of Europe Convention on Cybercrime

http://www.smh.com.au/federal-politics/political-opinion/cyber-law-casts-the-proper-net-20110829-1jib6.html
http://theconversation.com/cybercrime-bill-makes-it-through-but-what-does-that-mean-for-you-8953

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2015

ISPs and telcos required to store metadata for 2 years

- Sender, recipient, time (e-mail)
- Sender, recipient, time (phone calls)
- IP (DHCP)
- Info available (on receipt of a warrant) to Aust LE, US NSA and UK GCHQ

Not collected: organisation-wide e-mails, YouTube, Skype, Gmail, Hotmail

http://www.smh.com.au/federal-politics/political-news/senate-passes-controversial-metadata-laws-20150326-1m8q3v.html
http://www.abc.net.au/news/2015-05-08/edward-snowden-says-australias-mass-surveillance-dangerous/6456938

PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017

- Starts in Feb 2018
- Businesses must report data breaches to customers
- Tell them what to do (delete, pray, update)
- Fines $360k

https://www.itnews.com.au/news/australia-finally-has-mandatory-data-breach-nofitication-450923

SWINBURNE UNIVERSITY OF TECHNOLOGY

FUTURE DECRYPTION LAWS (AU)

- **Force Apple, Google, Facebook to decrypt user's traffic for law enforcement agencies**
- **Hotly debated**
- **Weakens security**
- **Intended that Apple, Google, Facebook provide info; no instructions on how.**

https://www.gizmodo.com.au/2017/07/australias-planned-decryption-law-would-weaken-cybersecurity/

http://theconversation.com/australias-planned-decryption-law-would-weaken-cybersecurity-81028

US LAWS

DMCA (1998)

- Protects copyright owners
  - Prevents fair use

- Makes bypassing copy-protection schemes (incl. encryption) illegal
  - Reverse engineering crypto is illegal
  - Studying crypto is illegal
  - Backups are illegal

US LAWS

USAPatriot Act (2001)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

- US Goverment. allowed to monitor its citizens
  - Internet taps
  - Phone taps
- No probable cause requirement
- Intelligence sharing allowed
- Voice mail reclassified as data (not a phone tap)
- Carnivore to be deployed at ISPs
  - black box which searches web traffic for keywords and reports users who type/read them

US LAWS

Cyber Security Enhancement Act (2002)

- Police/government agencies allowed to phones/networks without a warrant
- ISPs allowed to hand over customers' private data / logs
- ISPs allowed to let police tap their networks

US LAWS

2003 CAN-SPAM Act

- Spam is legal as long as
  - Sender's name, address not false
  - Spam says it is commercial
  - Opt-out option
  - No relays, porn, brute force/dictionary
- US States prevented from introducing tougher laws
- Spam volume increased under this law

US LAWS

Cyber-crime Act (2007)

- Conspiracy now an offence
- Minimum 10 computers before action is illegal
  - Illegal action used to be based on min $5k damage, changed to 10 computers.
  - Protects owners of zombies
  - Exposes Bot-Herders to prosecution
- Cyber-extortion added to list of crimes

US LAWS

2008

CAN-SPAM updated

- Sender better defined
- designated sender responsible for opt-out
- physical address now includes PO boxes
- Person redefined to include corporations
- Dedicated opt-out web page

US LAWS

Cybersecurity Act (2009)

President can declare a cybersecurity emergency

- Shut down internet traffic [sic]
- Sec. of Commerce has power to access anything regardless of privacy laws.

US agencies fighting over who is in charge of cybersecurity.

CYBERSECURITY INFORMATION SHARING BILL (2014)

- **NSA having access to even more personal data**
- **facilitate cyber threat and attack information sharing between government and private sector companies. Must be de-identified**
- **The problem is that once the data are in the government's possession, there is a considerable amount of leeway in how it can be used**

http://www.nationaljournal.com/tech/a-new-cybersecurity-bill-could-give-the-nsa-even-more-data-20140627

[Editor's Note (Murray): One need only consider the source. This bill is not about cyber security but about intelligence.]

DEPARTMENT OF DEFENSE APPROPRIATIONS ACT 2015

Funding for NSA to add back doors to equipment cut

http://www.cnet.com/au/news/house-oks-measure-defunding-nsa-backdoor-surveillance/

CHINA CYBERSECURITY LAW

Allows China Government surveillance of commercial activities, tech companies.

- **Legalises what they do anyway.**
- **Opposed by US, AU businesses.**

https://www.itnews.com.au/news/china-to-implement-controversial-cyber-security-law-463468

SOMETHING TO THING ABOUT

Are:

Employers now permitted to read employees' e-mail / web without consent?

Is this only spying agencies / police ?