

# Lawful Interception

Andres Rojas

Centre for Advanced Internet Architectures  
Swinburne University of Technology

anrojas@swin.edu.au

Feb 9th, 2006



## Outline

---



- My Background
- What is LI?
- LI in Australia
- History of LI
- Right to privacy and Lawful Interception
- State of play: e-mail, SMS, VoIP
- How is telephone interception carried out?
- How is IP-based interception carried out?
- Abuse
- Our Research
- Conclusion

## My Background

---



2000 - 2003 :

- Software Engineer : Lawful Interception Management Application for mobile telephony networks - Ericsson

2004 - :

- PhD Candidate : studying lawful interception in IP based networks - Center for Advanced Internet Architectures, Swinburne University of Technology

## What is Lawful Interception (LI) ?

---



"the lawfully authorised interception of a subject's communications and it's delivery to a Law Enforcement Agency"

- legislation to protect the privacy of individuals by making it illegal to intercept someone's telecommunications - except if you're authorised
- a tool for the collection of evidence in criminal investigations
- aka "Wiretapping"



- Telcos & ISPs have obligations with regard to law enforcement:
  - ISPs must give reasonable help to agencies for enforcement of criminal law
    - customer details
    - message source, destination
    - log files
  - prevent their infrastructure being used for crime
  - ensure their network is able to intercept communications passing over it
- failure in complying with these can mean their license is revoked, or heavy fines imposed.

## Lawful Interception in Australia

---



The *Telecommunications (Interception) Act 1979* (the Interception Act), 2 objectives :

1. to protect privacy of individuals who use the telecommunications system by making it an offence to intercept communications passing over that system other than in accordance with the provisions of the Interception Act
2. to specify the circumstances in which it is lawful for interception to take place:
  - ... under the authority of a warrant - by law enforcement agencies for the investigation of serious offences, or by ASIO for national security purposes.

## Lawful Interception in Australia (2)

---



The Interception Act defines 'interception' as:

listening to or recording, by any means, a communication in its passage over the telecommunications system without the knowledge of the parties

## Lawful Interception in Australia (3)

---



- Agencies include:
  - Australian Federal Police (AFP), Australian Crime Commission (ACC)
  - State police bodies
  - State anti-corruption commissions
  - ASIO <sup>1</sup>
- Crimes of interest:
  - narcotics offenses, murder, kidnapping, terrorism, corruption
  - aiding, abetting and conspiring to the above
  - offenses involving loss of life, serious injury, serious arson, drug trafficking, serious fraud, child pornography, people smuggling, offenses involving planning and organisation
  - an offense that is punishable by imprisonment for at least 7 years

---

<sup>1</sup>ASIO Act 1979 - gather information, produce intelligence for protection of national security

## Lawful Interception in Australia (4)

---



Lawful Interception warrants:

- may be applied for only by eligible authorities
- may only be issued by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member :
  - declared by Attorney-General to be eligible,
  - in 03-04 included judges from Federal Court, Family Court and Federal Magistrates Court
  - in granting warrant gravity of conduct, degree of interference with privacy and alternative ways of investigation must be considered
- normally, application for warrant must be in writing
  - for urgent cases, application is made by telephone

## Lawful Interception in Australia (5)

---



Safeguards and Controls:

- AFP and ACC required to maintain records relating to interception; Ombudsman to conduct regular inspections of records
- AFP must submit a General Register of Warrants to the Minister (AG) every 3 months detailing all warrant in force during that period
- AG kept informed of all agencies' activities by reports from agencies and Ombudsman
- parallel State legislation - a precondition to AG authorising state agencies
- the Telecommunications Interception Division of the AFP : supervisory control over the execution of all interception warrants

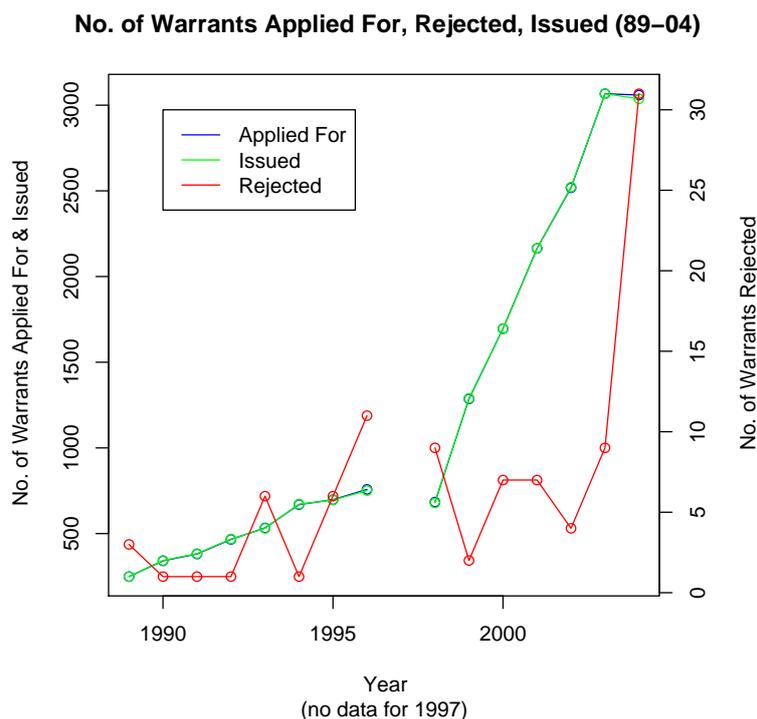
## Lawful Interception in Australia (6)



### Accountability:

- Commissioner of AFP maintains General Register and Special Register : inspected by AG, Ombudsman
- copies of warrants and reports on outcomes of interception : given to AG and/or responsible State minister
- Managing Director of carrier must report to AG about nature and timing of acts done by employees
- Commonwealth Ombudsman inspects records of AFP and ACC, reports to AG. State Ombudsman inspects state agencies, reports to state minister, copy to AG
- Annual report by AG tabled in Parliament

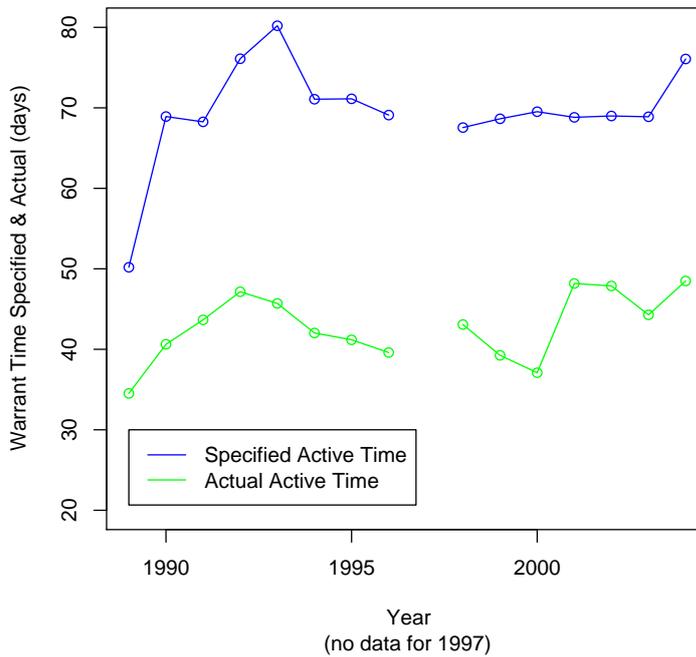
## Lawful Interception in Australia (7)



# Lawful Interception in Australia (8)



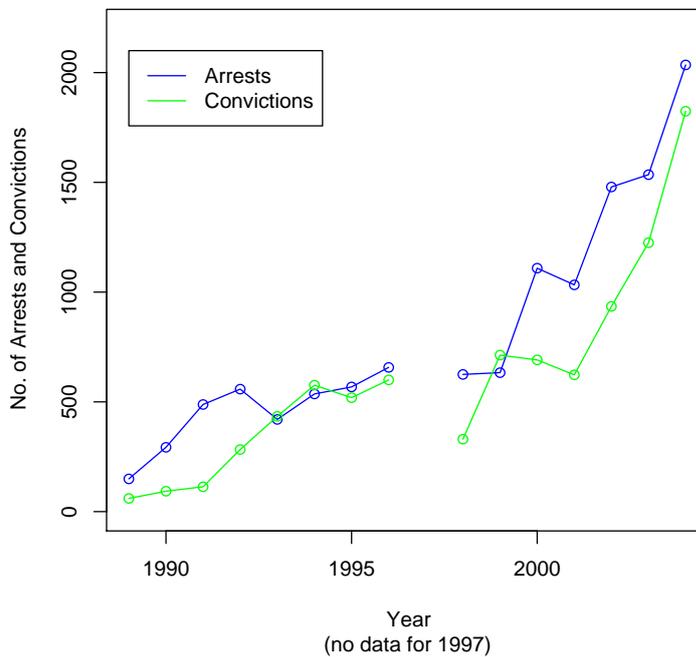
### Warrant Time Specified & Actual (89-04)



# Lawful Interception in Australia (9)



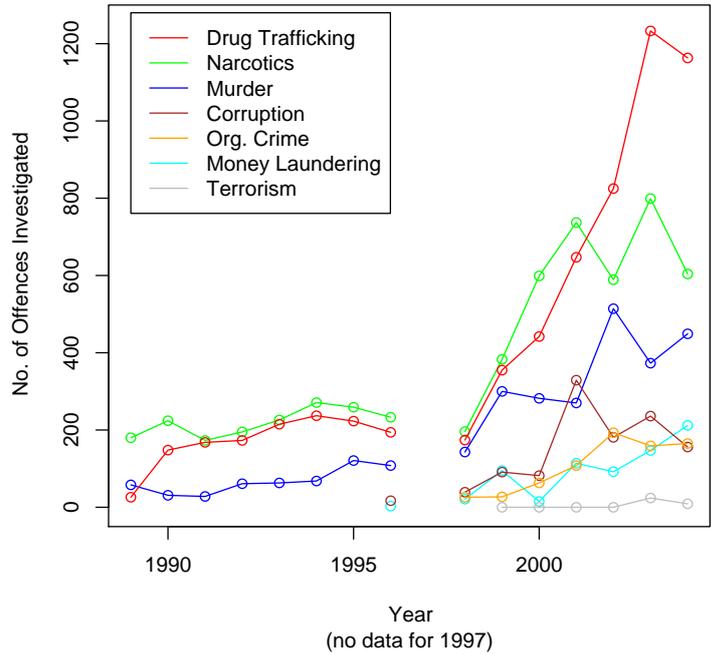
### Number of Arrests & Convictions (89-04)



# Lawful Interception in Australia (10)



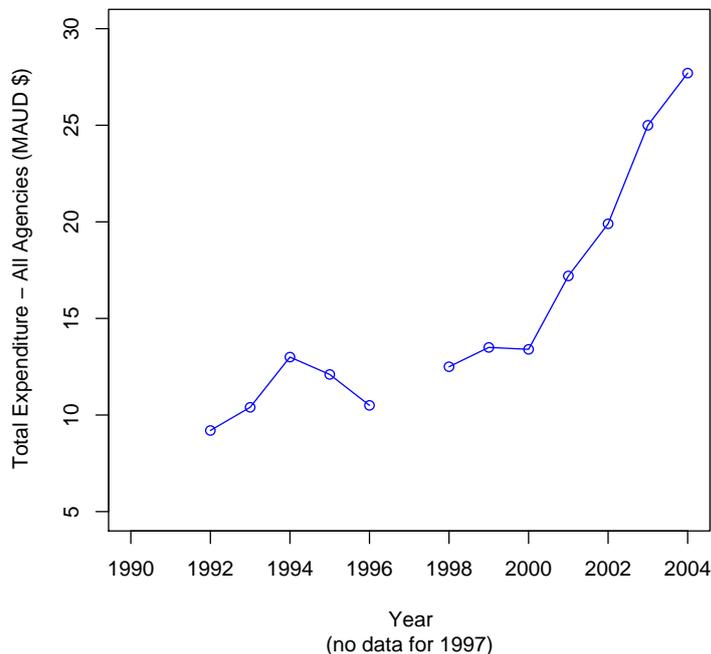
No. of Offences Investigated using LI (89-04)



# Lawful Interception in Australia (11)



Total Expenditure on Lawful Interception (92-04)



## History of Lawful Interception - Legislation

---



- Summaries:
  - Chan & Camp, [2], provide a good survey of the history of LI in the U.S.
  - Russell Smith, AIC, [1], provides a summary of the history of LI in Australia.
- In Australia:
  - Oliver Cromwell's law of 1657 : state monopoly on postal mail
  - *Federal Communications Act 1934* : restrict the use of intercepted communications
  - *Telephonic Communications (Interception) Act 1960* : regulate the interception of telephone comms.
  - *Telecommunications (Interception) Act 1979* : wiretapping - listening/recording of comms in the system.
    - comms carried solely by radio communications - may be intercepted
    - bugging (*Surveillance Devices Bill (2004)* - passed), spying, hacking, EM scanning

## History of Lawful Interception - Research

---



Denning, [3] :

- early 90s:
  - emergence of new digital voice and data services
  - LI methods at the time were only designed to intercept analogue voice
  - ability of law enforcement to gather evidence was at risk
- U.S. Dept. of Justice proposed legislation to require network operators to maintain their ability to intercept
- Denning presented the case for the legislation and argued against opponents' concerns

## History of Lawful Interception - Research (2)

---



- Opponents cited concerns that the legislation would:
  - hold back technology innovation as interception had to be considered in new designs,
  - lead to uncompetitive U.S. products
  - introduce security holes that would severely undermine the public's right to privacy
  - be costly to implement. An unjustifiable cost.
- Denning introduced the idea that the shift in balance towards absolute individual privacy is in itself a threat to security:

*"The consequence of this choice will affect our personal safety, our right to live in a society where lawlessness is not tolerated, and the ability of law enforcement to prevent serious and often violent criminal activity."*

## History of Lawful Interception - Research (3)

---



Chan and Camp, [2] :

- provide a framework for the implementation of government LI policy for data protection, privacy, and surveillance,
- introduce the critical ideas that:
  - it would not be in the broader community's interest to leave LI system implementation solely in the hands of government agencies: telecomms industry should assist law enforcement with LI needs
  - implementation of LI should be subjected to scrutiny, open source development should be aggressively encouraged : guard against mistaken interception via a robust system.



- Interception Act claims that the legislation protects the public's privacy by making interceptions of communications illegal (except for the exceptions)
- Is this our only recourse ?
- other tools exist to guarantee our privacy (and foil lawful interception in the process)

## What about Encryption ?

---



- Warrant specifies: Content of Communications, AND/OR, Meta-data about Communications (signalling)
- "majority" of warrants specify meta-data ONLY !
- There is value in meta-data:
  - who is talking to who,
  - at what time is communications taking place,
  - where was Alice when she talked to Bob
  - increase in frequency = planning
  - communications to a central location = hierarchy



- Anonymity, protection against traffic analysis :
  - Tor, onion routers : circuit set up one hop at a time, encrypted, random paths (tor.eff.org)
  - Freenet : comms are encrypted, routed through freenet nodes. Difficult to detect who is requesting what (freenet.sourceforge.net)
  - I2P : I2P router builds outbound & inbound tunnels = network of relaying peers (i2p.net)
  - IPv6 address privacy extension : devices are traceable, MAC based addresses - never change. Make them vary over time. (RFC 3041)



- Stored Communications Amendment to Interception Act :
  - passed by Aus. Senate Nov 2004
  - removes protection from interception for email, SMS, voice mail messages that have not been delivered
  - since protection is removed, allows anyone to intercept these without a warrant
- US DoJ, Nov 2005, wants legislation extended to handle VoIP interception
  - for calls to or from the PSTN
  - Skype says : "many VoIP products are used not to replace traditional telephony, but as a component of electronic messaging and other information services ..."
- Data retention laws passed in EU (12-36 months)

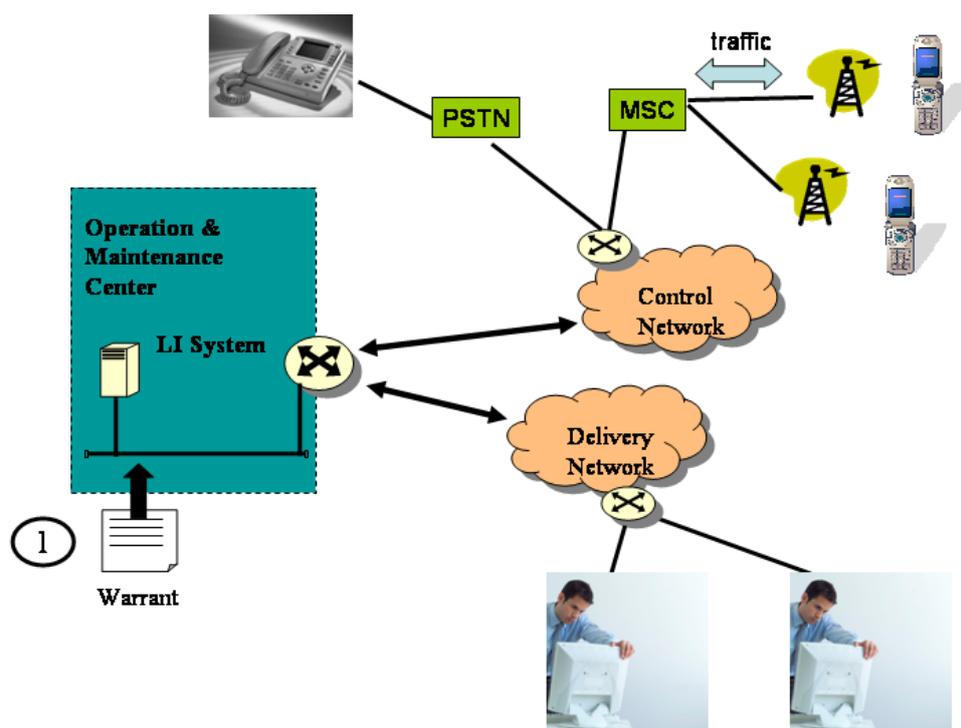
## How it works : telephony



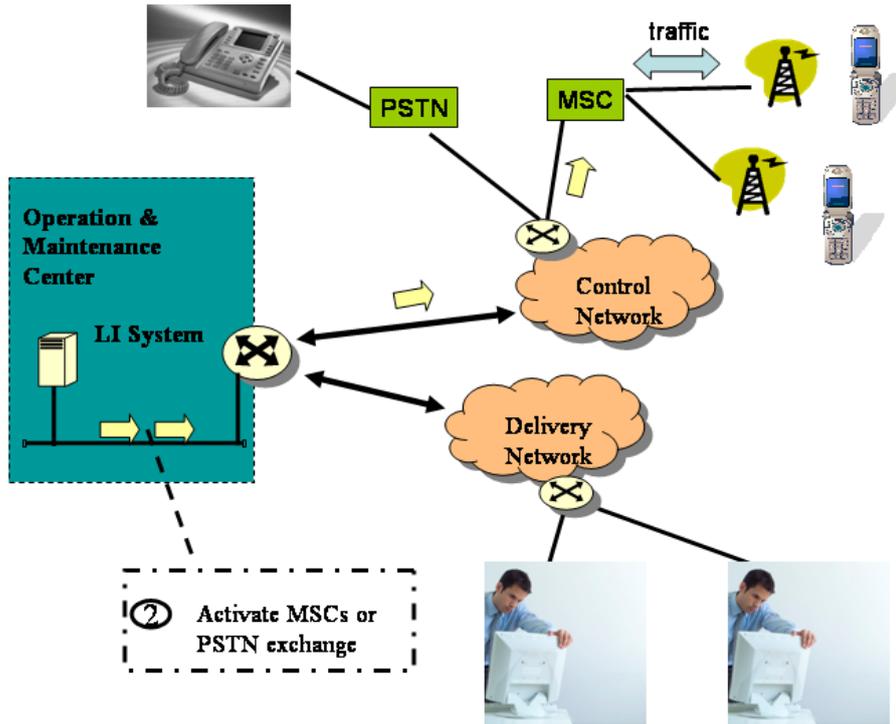
- Loop extender taps : most basic and oldest method <sup>2</sup>
  - local loop connection
  - 2nd connection (circuit) made to the law enforcement agency
  - fixed line telephony only
  - still used
- Managed interception.

<sup>2</sup>Vulnerabilities found - Nov 2005 - <http://www.crypt0.com/papers/wiretapping>

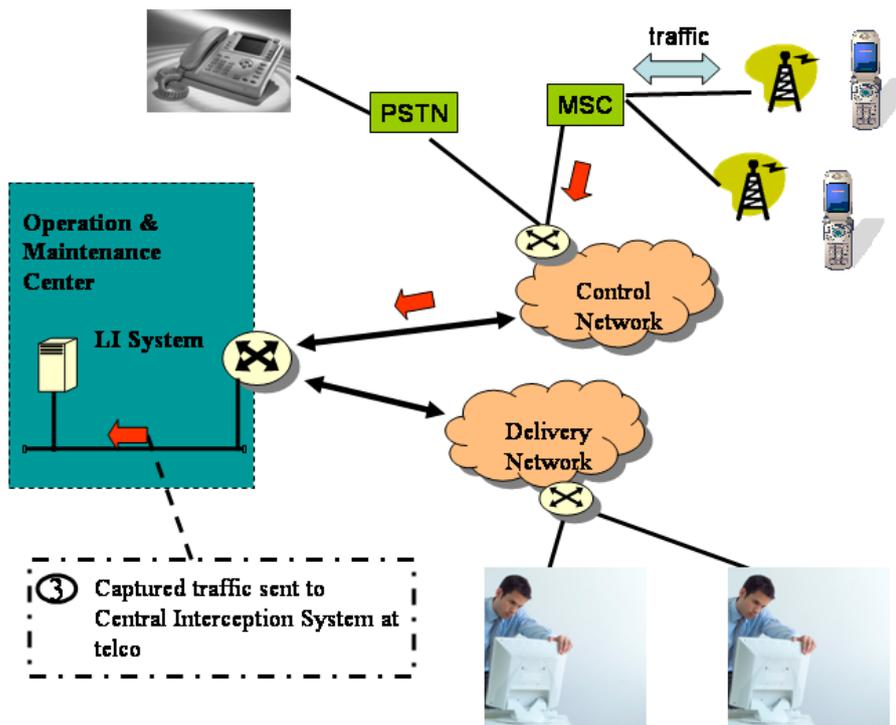
## How it works : telephony



# How it works : telephony



# How it works : telephony







Detailed by Smith, [1], cases where interception is unlawful :

- by Law Enforcement Agencies:
  - 1967-1983 illegal telephone interceptions by NSW police. At direction of Commissioner. Over 200 interception operations. (Stewart Royal Commission 1986)
  - alleged illegal interception by NSW police of telephones of various bookmakers. (Wood Royal Commission 1996)
  - Interception almost always complied with Interception Act. No intentional abuse, just inexperience, lack of training (Barrett Report 1994)
- by Private Individuals:
  - cases involving installation of interception devices to obtain information to discredit witnesses.
  - industrial espionage : AFP found interception devices on telephones of Holmes a Court, Burrows (stockbroker), and McCrann (journalist) - allegedly arranged by Bond Corp. (1990)
  - discretion of court : infringement of Interception Act, Listening Devices Act.



- Carnivore (aka DCS1000) was FBI's in-house developed Internet interception application :
  - deployed at ISP premises. Packet Sniffer and off-site analyser. Windows 2000 based.
  - potential for abuse :
    - FBI never released source code
    - extent to which Carnivore complied with regulation unknown.
    - Suspicion : what is it really doing? (PR/openness problem)
  - FBI now prefers off-the-shelf solutions



- Verint of Israel (formerly Comverse-Infosys)
- supplier of interception solution for telephony & Internet to Dutch Gvmt
- *allegedly* thought to have a backdoor to Israeli intelligence service
- *allegedly*, Dutch gvmt got reduced price in exchange for access to tapped information
- Verint tech staff perform *maintenance*, leave with drives full of data.

## Our Research

---



Centre for Advanced Internet Architectures at Swinburne University of Technology :

- Lawful Interception For Everyone (LIFE)
  - robust and secure techniques for Lawful Interception requiring minimal introduction of new hardware
  - Lawful Interception of emerging networks and technologies
  - Techniques for harmonizing access network and IP network Lawful Interception obligations
- Meet competing demands of :
  - Law Enforcement - who need access to specific traffic, and
  - User expectations - that interception will not exceed the levels allowed by law, nor unreasonably weaken the Internet's overall security



Example of our Research - Use of Sniffers in Next Generation Networks, [4]

- current use of traffic sniffer to detect traffic from/to a certain IP address
- RADIUS based - to detect what IP address is allocated to a certain user
- newer networks : IPv6+RADIUS, DIAMETER based, MobileIPv6+AAA
- stricter demand for security - no more cleartext
- means further complication for LI systems

## Conclusion

---



- Definition
- Legislation in Australia
- History
- Privacy : protecting Privacy
- State of play : email, SMS & VoIP
- How it works : telephony & Internet
- Abuses : agencies & individual
- Our Research



- Bruce Schneier ([www.schneier.com](http://www.schneier.com))
  - years ago : trenchcoats, following people down the street, labourious, expensive
  - now : more efficient, increasingly integrated ways to oversee/track people
    - aerial photos to detect building permit infractions,
    - security cameras are everywhere,
    - transactions tracked by banks, calls tracked by phone co., web surfing by web site operators : surveillance backwards in time
    - automatic licence plate scanner
- Critical idea :
  - How much privacy to give up for security ? , should be
  - what mechanisms are in place to prevent abuse ?



---

## References

- [1] Controlling the Interception of Communications: Law or Technology. "Communications Research Forum, Canberra", October 1997.
- [2] S. Chan and L.J. Camp. Law Enforcement Surveillance in the Network Society. *IEEE Technology and Society Magazine*, 21(2):22–30, 2002.
- [3] D. Denning. To Tap or not To Tap. *Communications of the ACM*, 36(3):24–33, March 1993.
- [4] Andres Rojas and Philip Branch. Lawful Interception based on Sniffers in Next Generation Networks. In *Proceedings of the Australian Telecommunications Networks and Applications Conference 2004*, December 2004.