Privacy

Lee Naish
Computing and Information Systems

Outline:

- What is privacy?
- Privacy and computers/the internet/the web
- Information Privacy Principles, Legislation
- Practice

What is privacy?

"The right to be left alone"

Privacy versus secrecy

Balance with "the right to know", "freedom of information"

Cultural expectations, eg:

- electoral role
- property and other ownership
- political donations
- tax records
- library/video/dvd loans

Computers and privacy

Computers were initially thought of as calculating machines

The ability of computers to store, search, sort and collate information quickly and cheaply has been at least as revolutionary and has profound implications for privacy

Unique identifiers make it easier to combine different sources of information about people/households

Eg, student number, credit cards, phones, Medicare number, Tax File Number, SSN, login id, IP address, computer chip id, cookies, ...

The internet/web and privacy

Computers are now the key to communication (eg, communicating information about you to the rest of the world)

We interract directly with computers much more now; mostly on the web (buying stuff, social networking, entertainment, work, getting on with our lives). There are no "data entry" costs.

Authentication are is more based on what we know, ie, information (rather than what we have or what we are)

Why are we losing our privacy?

People want our money:

- The spam we get (and junk mail and phone calls, etc)
- The advertisements you see when you use the web
- Identify theft of various forms (eg, phishing)

Governments have a tendency towards being "Big Brother"

Concern over privacy has been around a long time

- Mid 1970's: OECD privacy guidelines
- 1975–early 1980's: Privacy committees in NSW, Qld, SA
- 1980: International Covenant on Civil and Political Rights ratified
- 1986: Privacy Bill + "Australia Card" proposed
- 1988: Commonwealth Privacy Act (+ Tax File Number)
- 1994: Australian Privacy Charter
- 2000: Victorian Privacy Act
- 2000: Commonwealth Privacy Act ammendment

Information Privacy Principles

Victorian Information Privacy Act, 2000 has IPPs:

1. Collection: only necessary data, not intrusive or unlawful, inform individual why, who to contact, ...
2. Use and Disclosure: consent, anonymous, safety, law, ASIO, ..., record disclosure
3. Data Quality: "reasonable steps"
4. Data Security: "reasonable steps", destruction of data
5. Openness: policies, kind of data, ...

Information Privacy Principles

6. Access and Correction: access/update by individuals unless . . .
7. Unique Identifiers: consent, "efficiency", outsourcing; nondisclosure, purpose of identifiers
8. Anonymity: an option when lawful and practicable
9. Transborder Data Flows: consent, same privacy principles apply
10. Sensitive Information: not unless consent, law, safety, . . . but ok for welfare, education, no alternative

So everything is fine, right?

Clearly not . . . (see epic.org, privacy.org)

The first aim of the Victorian Information Privacy Act is "to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information *in the public sector*"

The Commonwealth 1988 Privacy Act since the 2000 ammendment has applied to the private sector but there are many exemptions, eg information can be disclosed for direct marketing

Outside the boundaries of Australia (eg, the internet) you have no control of where your personal information goes

There is a *huge* quantity of personal information collected, and collated with other information

Privacy versus commerce

Most commercial Web sites collect personal information (IPP 1?)

They generally have an official privacy statement (IPP 5)

Some promise not to disclose information to third parties (IPP 5, 2)

And its not just web sites collecting information

"Spyware" applications collect information on their usage and "phone home" occasionally

Pretty much every time a card is swiped, data is collected

Some goods have RFID (radio frequence identification) tags which can be used to track their use after you buy them, and information from Bluetooth-enabled devices is collected, etc

Cookies

Cookies are data stored on your computer which are used to track your browsing

Many sites contain advertisments (links to images) which originate from a central site (eg, DoubleClick)

An (old) example: Searching for "privacy" on lycos.com got me to the URL `http://www.lycos.com/srch/?lpv=1&loc=searchhp&query=privacy`

This (generated) page contained an image whose source was at `http://ln.doubleclick.net/ad/ly.ln/r;kw=privacy;pos=1;sz=468x60;tile=1;ratio=1_2;ord=816238249?`

When the browser loads this image, it also gets a cookie from DoubleClick and stores it locally

Each subsequent time the browser loads something from `ln.doubleclick.net/ad` it sends the cookie to DoubleClick

Cookies

After visiting the Melbourne Uni home page and BOM Melbourne weather forecast page you get cookies from unimelb.edu.au and bom.gov.au (unsurprisingly), but also youtube.com and adnxs.com

If you are logged in to a GMail account you also have youtube.com cookies and Google knows who you are and what you are viewing. Such information is used by Google to build up a profile of you

According to an article in The Guardian about sites which track browsing, adnxs.com is also one of the top ten tracking sites worldwide

Ironically, viewing that article online results in cookies from 26 different domains being stored by uour browser!

Privacy versus commerce

Sometimes there is something in it for you, eg

- "enhanced browsing experience"
- e-mail
- social networking
- software
- fly-buys
- cash back offers
- discount cards
- return of your lost Myki card
- ...

But be aware that these benefits are paid for using personal information (IPP 8)

Consent versus informed consent

Information privacy principles say anything is ok with your consent

But privacy statements are often not prominent

They are written to satisfy lawyers rather than inform the public

Many people are not aware of what information is collected and what is done with it

Sometimes companies behave badly...

They change their privacy policies without warning (Facebook, Google, ...)

or just don't comply with their own stated privacy policy (Facebook, Google Buzz, ...)

or have "serious lapses in their security" (Twitter, ...)

or just blatantly flout the law (Google streetview, Echometrix, ...)

Often they get away with it

We have a Victorian Privacy Commissioner but he can't do much

Some advice...

Constant vigilance is needed to maintain privacy

Value your privacy (if you still have any)

Value your kids' privacy (if you have any)

If you have lost your privacy, try not to piss anyone off

How did we get to this state?

The internet was created by people who were mostly funded by governments, from taxation

Since the late 1980's, free market capitalism has been the dominant force, with relatively minor government regulation (in most countries)

Although markets are an efficient mechanism for producing many kinds of goods, they are not an efficient mechanism for building infrastructure, or for information goods

Economists use the term "market failure"