

# **Privacy, The Law and Global Business Strategies**

## **A Case for Privacy Driven Design**



**Mary-Anne Williams**

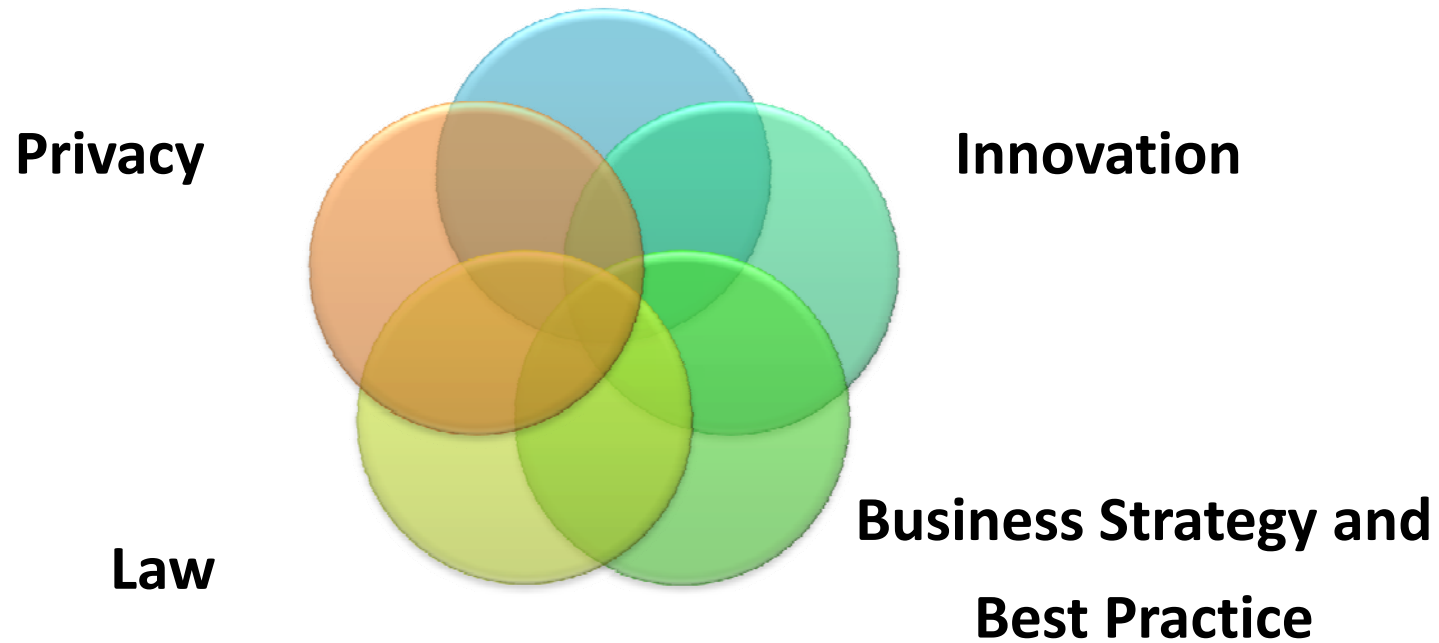
Innovation and Enterprise Research Lab  
University of Technology, Sydney Australia  
*Mary-Anne@innovationlawcentre.org*



# Global Contemporary Business



## Business Opportunity and Competition





# Privacy Law

*"Privacy law is **not** the product of **logic** ... nor for that matter is it the product of **experience**.  
It is the product of **local social anxieties**  
**and local ideals.**"*

James Whitman

2004



# IT is intertwined with Privacy



- Prosumerism, e.g. Trip Advisor
- Web 3.0
  - Socialization, e.g. Twine, Chi.mp,
  - Innovative Semantic Services
    - Web Services
    - Geolocation Services
    - Recommender Services
    - Other service models ...
  - Pattern Discovery via Data Mining
  - Appvertising – embedding advertising in services/games



# Overview



- Background
- Privacy
- The Law
- Key Concepts: Consent, Choice, Control
- Challenges Ahead for Privacy Management
- A possible way forward
- Discussion



# What is Privacy?

- Privacy is a complex cultural context-based social and legal concept.
- The **right** to be left alone and the **right** to be free of unreasonable personal intrusions – 19<sup>th</sup> century Common Law interpretation – [Warren and Brandeis 1890]
- The expectation that **confidential personal information disclosed in a private place will not be disclosed to third parties**, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. *Information* is interpreted broadly to include facts, images (e.g., photographs, videotapes), and disparaging opinions. [Standler 1997]
- In the global economy privacy is a global legal and social challenge because **information is collected in one jurisdiction is often processed in another jurisdiction.**



# International Law



- 1948 the UN adopted the Universal Declaration of Human Rights
  - *No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*



# Privacy and US Law

- The US was the first country to focus on privacy as a public issue – 1960s
- Federal Legislation on credit records
- Watergate exposed abuse of government data
- Privacy Act 1974 governs admin records held by Federal Agencies
- Currently piecemeal law covering personal data in health care, bank records, video rentals etc





# US Constitution

## First Amendment



- Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; **or abridging the freedom of speech**, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.



# The USA Patriot Act



- E-mail and Internet searches
- Nationwide roving wiretaps
- Requirement that ISPs hand over more user information
- Expanded scope of surveillance based on new definitions of terrorism
- Government spying on suspected computer trespassers with no need for court order
- Wiretaps for suspected violations of the Computer Fraud and Abuse Act



# The USA Patriot Act

- Dramatic increases in the scope and penalties of the Computer Fraud and Abuse Act
- General expansion of Foreign Intelligence Surveillance Act (FISA) authority
- Increased information sharing between domestic law enforcement and intelligence
- FISA detours around federal domestic surveillance limitations; domestic surveillance detours around FISA limitations



# Privacy Law in the USA



- **Focuses on Government** data collection
- On the business side – virtually a **free market** – little protection for individuals
- **Fragmented** across the states – e.g. 1988 Video Privacy Protection Act created in response to a newspaper publishing the video rental records of Judge Robert Bork during Supreme Court hearings concerning his nomination.
- **Not principles based** and not future technology proof
- **Does not comply with the EU Directive** and transatlantic information transfers are a special and temporary exception (a so-called safe harbour).



# US Uniqueness/Quirkness



- No National Agency for Privacy
- Piecemeal privacy law, not broad rights, in the private sector
- Many forms of private sector data in the US are not governed by any rights to individuals
- Individuals must act on their own behalf to enforce their privacy rights
- No omnibus privacy rights – rights over all (or nearly all) categories of personal information
- Impact of The War on Terror, e.g Air travellers private information made available to US authorities.
- US Law strongly influences global trends – some have argued that this has led to the serving of private interests and an erosion of privacy



# Personal Info Protection in Other Countries



- In 1998, the European Union passed a privacy directive (EU Data Protection Directive) sets out principles of personal data protection across the board.
- The EU directive aims to regulate the activities of any person or company that controls the collection, storage, processing, or use of personal data on the Internet
- Australia's Privacy Laws are principles based and currently under review
- Privacy law is under construction in most countries in Asia e.g. China (except for Hong Kong)



# Influential Codes of Practice



- US Dept of Health, Education and Welfare 1973
- Council of Europe 1981
- OECD 1980
- Australian Privacy Charter Council 1992
- Canadian Standards Association 1996



# International Privacy Observers and Advocates

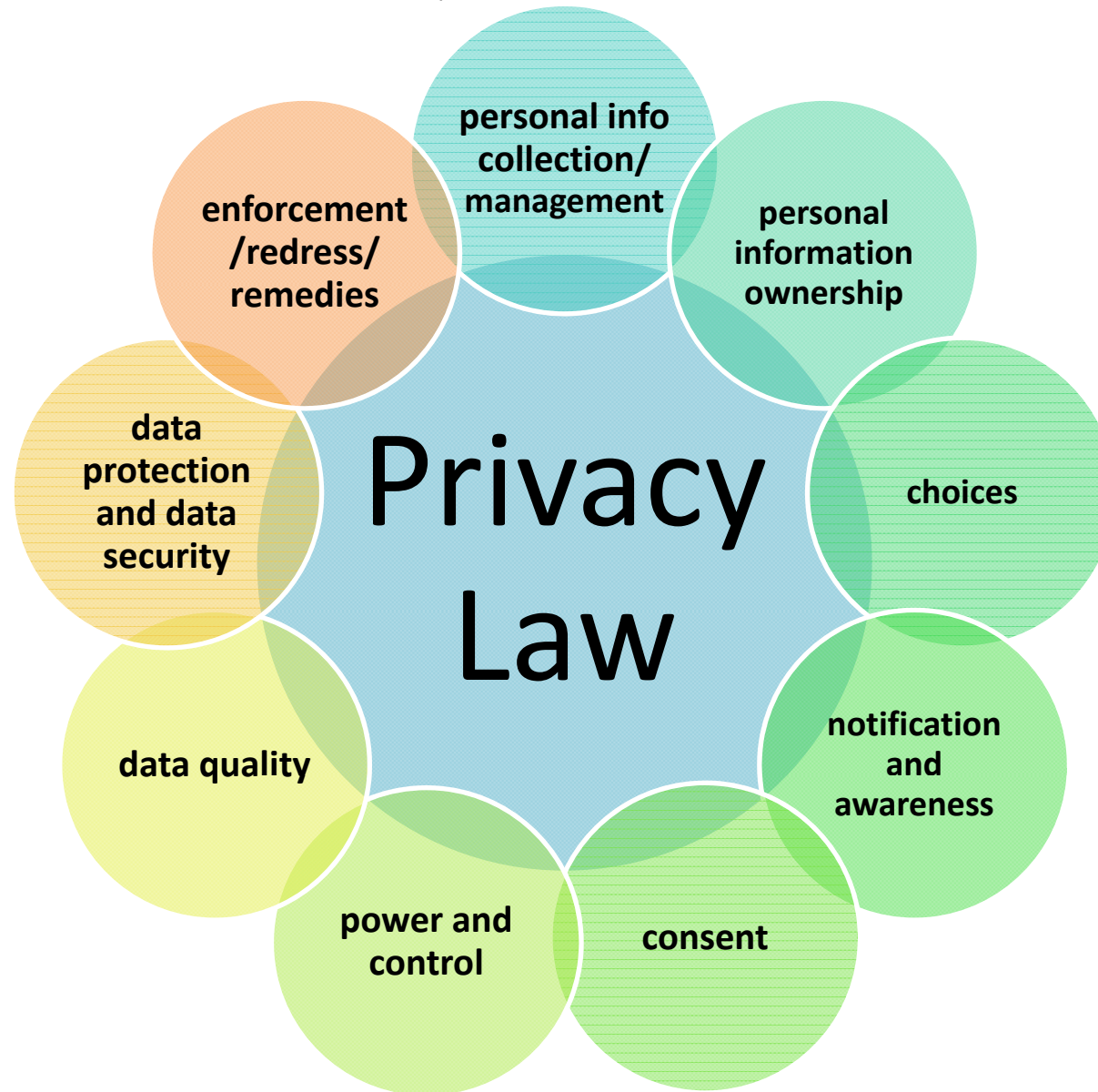


- Privacy International – London, UK
- EPIC – Washington, USA
- Option Consommateurs – Montreal, Canada
- A wide range of individuals – journalists, academics, informed and concerned citizens

But only **states** can create and enforce privacy codes.



# Privacy Law Issues





# Personal Information in Social Networks

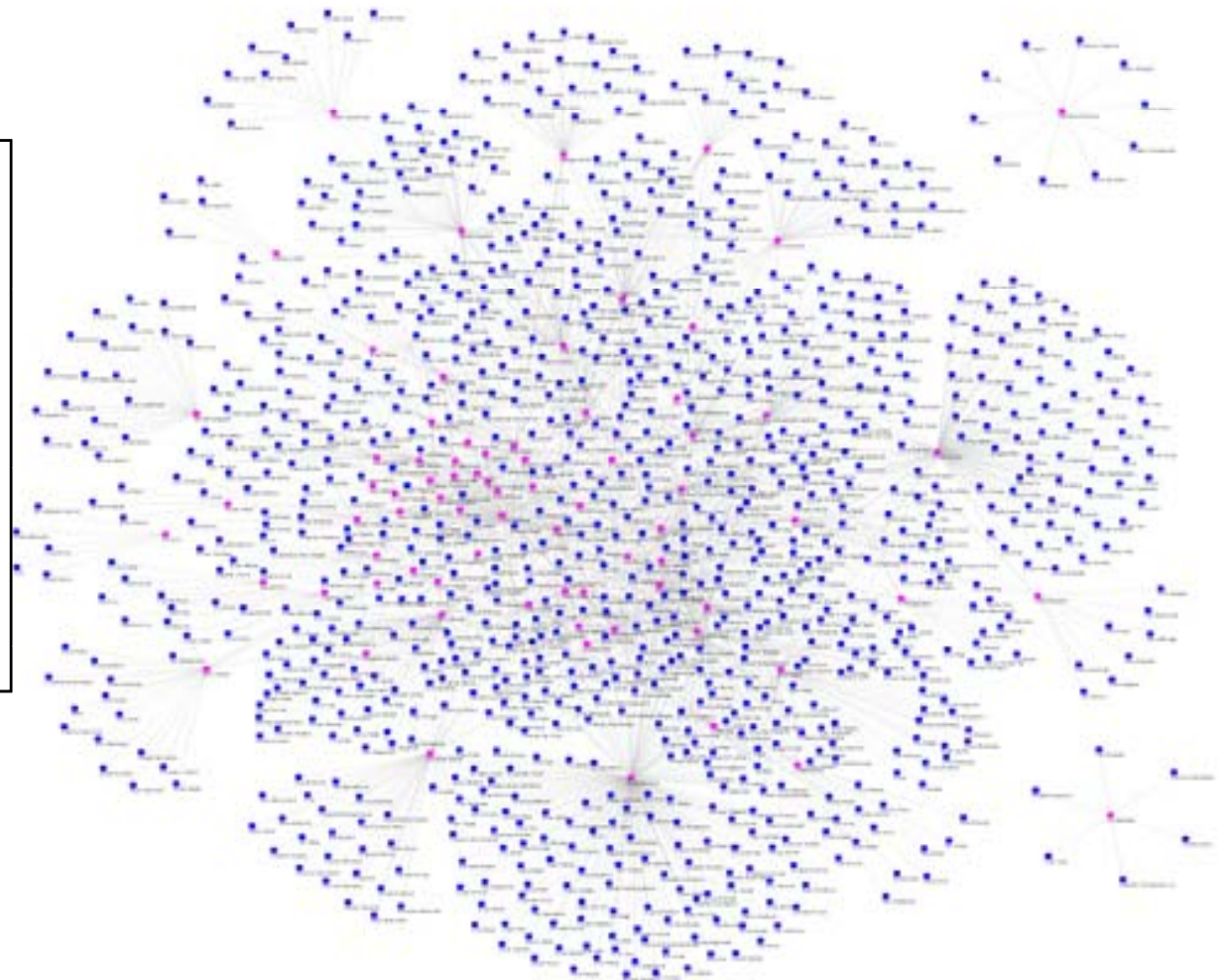


## User Profile

Name: Joe The Plumber

Age: 32

Address: Ohio





# Legal Status of Information on Social Networking Sites



- Governed by Contract Law
  - Privacy Policies
  - Terms of Use
- Related Law
  - Data Storage
  - Surveillance
  - Confidentiality
  - Freedom of Information



# Protection of Privacy



## Contracts

### **opt-out clause**

Agreement that requires computer users to take specific steps to *prevent* the collection of personal information

### **opt-in clause**

Agreement that requires computer users to take specific steps to *allow* the collection of personal information



# Facebook's Beacon Program



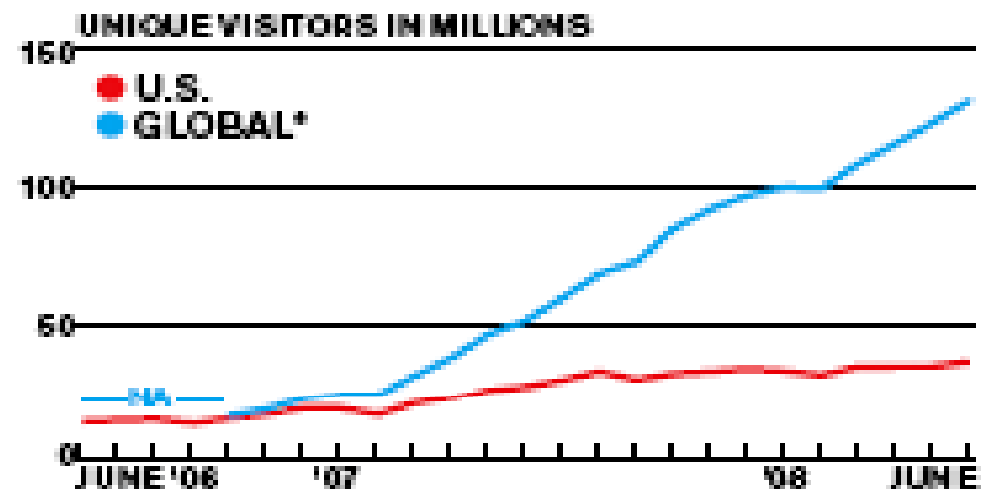
- Individual's activity on websites outside of Facebook is broadcast to other individuals (e.g ) within Facebook
- Introduced **without consent**
- *No more surprise gifts for partners and friends*
- No breach of law!
- There a huge backlash and Facebook had to rethink its strategy and practice

facebook



# THE TWO FACES OF FACEBOOK

U.S. growth is slowing, while worldwide increases are strong



Data: ComScore

\*WORLDWIDE INCLUDING U.S.



# Choice



- Scott McNally “**There is no privacy, get used to it**”
- Service Providers regularly **bundle consent** as a means to reduce the business burden and the burden of risk.
- Often they do not know themselves how they will use the personal information they collect in the future.
- Individuals are given **no choice** as to the particular uses or disclosures to which they are consenting.
- This raises the questions as to whether consent can be construed as freely given.



# Consent

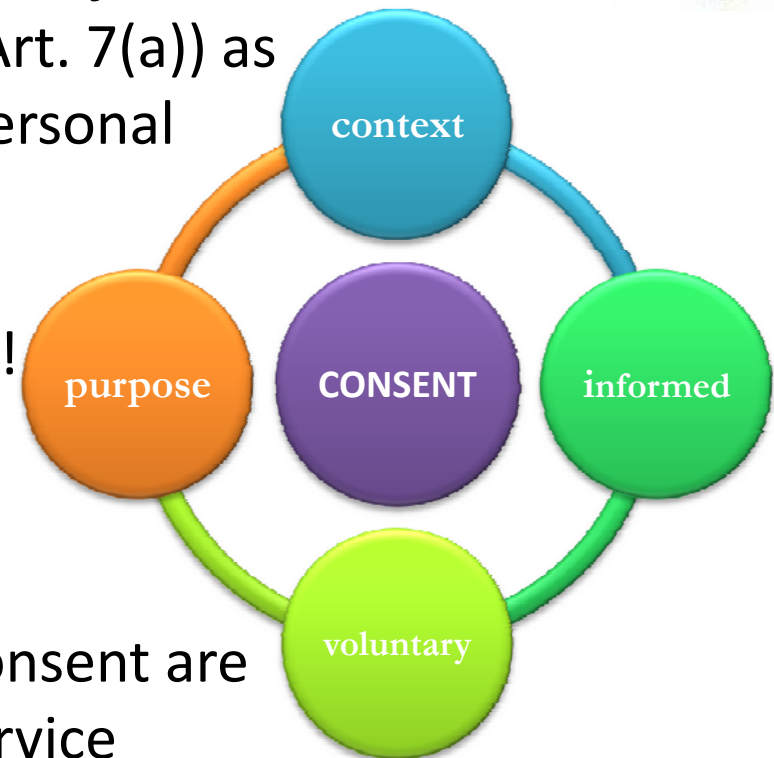


The EU Directive requires that “*the data subject has unambiguously given his consent*” (Art. 7(a)) as one of the bases for any processing of personal information.

Failure to opt out is not by itself consent!

Consent for uses and disclosures verses acknowledgement to conditions .

Acknowledgement of notification and consent are sometimes conveniently conflated by service providers.



*Case: Australian Communications and Media Authority v Clarity 1 Pty Ltd (2006) 150 FCR 494 – a Spam Act 2003*



# Control



- Awareness
- Notification
- Changes/Deletions



Professional Info



Professional Info

Friend Info



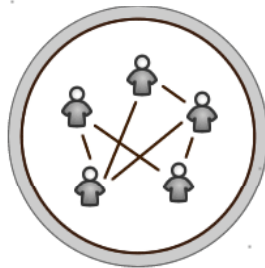
Professional Info

Friend Info

Private Info



myspace.com  
a place for friends



chi.mp  
OWN > EVOLVE



# Challenges Ahead

- The web is evolving rapidly and becoming increasingly rich and powerful.
- We all have a digital footprint that web applications can discover and exploit, e.g. behavioural targeting of users for products and services.
- New forms of business exploitation can lead to the disclosure of personal information, the invasion of privacy and subsequent harm.



# Future of Global Privacy Law



Given the difficulty in anticipating technological advances and their impact on innovation, privacy law should be technology neutral.

US law stands out as a laggard in the evolution of privacy law relative to the EU and emerging developments in Asia.

Given how far behind the rest of the developed world it is in protecting individuals personal information with respect to business practices in the private sector, the US needs to revolutionize its privacy law just to catch up. But will it?

Most of the next generation web services are and will be based in the US and as a result long term innovation could be compromised.

This situation creates opportunities for countries in other regions to develop competitive advantage by providing services that protect personal information in accordance with user expectations and requirements.



# Global Privacy Governance Future

- According to Harriet Pearson (2008) the Chief Privacy Officer at IBM privacy has become a source of consumer anxiety and corporate concern.
- Consumers are concerned and sometimes anxious that personal information can be exchanged, bought or sold for secondary use without their knowledge or consent.
- Consumers concerned about identity fraud, use of personal information on the internet, businesses sending personal information overseas for processing and the use of personal information for marketing.
- Privacy protection and enforcement are not only cultural issues in society, they are a corporate culture issues. Firms who understand the importance of maintaining their customers privacy in return for their loyalty have tended to last longer in the market place.



# Future IT Challenges for Privacy

- **Privacy is a local** phenomena while the **processing** of personal information **is global**.
- There are **competing drivers**: exploitation and potential for privacy violations versus enhanced customer service.
- Major **technology-enabled innovation trends that impact privacy** include data fusion, cloud computing, geo-location based services, and semantic web technologies
- **Example**: Plink an innovative social network had to close down due to the privacy issues created by its powerful information linking and integration engine.
- Plink's downfall clearly highlights the need for developers to take privacy more seriously by making its protection and enforcement a high priority in systems requirements.



# Opportunity for Leadership



- **What information needs is to be protected?**
  - Privacy? Clarity in requirements
- **What kinds of activities need to protect personal information?**
  - Profile info Management
  - Activity info Management
  - Propagating protection – sharing and integration across systems, businesses, and borders
- **What do we need?**
  - Community of Practice to develop a shared and visionary understanding
  - Solutions that
    - have low transaction costs for business
    - enable innovation and information flow
    - people can understand and use easily
    - scope for pro-active privacy management
    - are independent of technological change
  - Modelling tools
    - Privacy Representations
    - Privacy Management - reasoning
    - Simulations
  - Personal information protection patterns and templates





# Using Codes of Practice Common Themes as a First Step



1. The keeper of personal records is responsible.
2. The existence, purposes and workings of such systems should be readily accessible to public understanding.
3. A single figure should be publically identified as being responsible for safeguarding privacy interests.
4. Information must be collected legally and fairly.
5. Individuals must be able to review the content held about them , and the uses and disclosures . They must be able to obtain redress for inaccurate and inappropriate uses and disclosure.
6. Personal data should only be collected in the form and to the extent necessary to fulfil the purpose of the system.
7. Info should be accurate and current in order to fulfil the purpose
8. Info collected for one purpose should not be used or released for other purposes, except under legal requirement or with permission of the individual.
9. Info held should be collected with the knowledge or consent of the person concerned.



# Summary

- Privacy related law needs to be as robust to technological advances as possible.
- Changing U.S. Law as a means to improve global privacy law would be difficult
- Europe is essentially governed by the EU Directive and change will be slow
- Privacy Law in much of the world is still developing ... Asia has an opportunity to develop **privacy enabling law**
- New and improved Privacy Law needs to focus on **Choice, Control and Consent**
- **Innovation needs clarity and transparency in Law**, internationally competitive set-up and transaction costs to flourish.
- There is an opportunity for IT systems designers to show leadership in privacy and personal information protection.
- The law does not always lead and in IT related law it often lags, but it does catch up with societies expectations. If IT leads in the right direction and develops best practice approaches, then the Law may follow.