

“Data Protection: The Next 21 years? The operating environment”

Seminar hosted by the Information Commissioner, UK

Manchester, 29 November 2005

Malcolm Crompton

*Managing Director of Information Integrity Solutions, www.IISpartners.com;
Federal Privacy Commissioner, 1999 – 2004*

Introduction

The purpose of the seminar is to look at approaches to data protection as they have evolved, especially in the United Kingdom.

The purpose of this paper is to hang a backdrop to that discussion. It is deliberately intended to ask more questions than it answers and will at times push the boundaries of the comfort zone. Hence there are questions about radically changing the nature of data protection law and its role in the wider context of ‘doing the right thing’ about respecting people and the personal information about them. While there is necessarily an Australian focus in this paper, the conclusions equally apply in the UK, Europe more broadly, the US and most other advanced economies.

The paper is also optimistic. Most forecasts of the next 10 years are largely inaccurate, let alone forecasts about the next 21 years. Indeed, we can be certain that just as very few forecasts in 1990 predicted the impact of the internet by 2000, the world of personal information and its protection against misuse will be far more different than any of us predict at the moment. With care, vigorous debate, and a lot of hard work, we will still have private lives in 21 years time.

What is happening to our personal information?

The amount collected and range is growing explosively

“More information has been produced and stored in the past five years, than at any time in human history. E-mails, text messages, mobile phone calls, TV, websites. We are drowning in the stuff. But how much of it has added to the sum of human knowledge? And has anyone thought what it is doing to our brains? ... ‘I think you are going to see more rapid production of further information,’ says Keith Kendrick, head of neuroscience at the Babraham Institute, Cambridge.” So noted the BBC in 2003.¹

¹ “Reclaim your Brain”, BBC News, 3 November 2003, online at:
<http://news.bbc.co.uk/1/hi/magazine/3230665.stm>

This rate of growth is exponential. In other words, in 21 years' time, at this rate of growth, the information produced by then will be more than 16 times more than currently exists.

Much of the information collected is about each of us. It also includes very significant and potentially sensitive information, from our financial records to our health records with an increasing proportion of it subject to analysis in ways which many of us barely know about, ranging from credit histories to CRM or population health studies. To give some idea of what this means, one hospital has estimated that its data storage needs have increased nearly tenfold in the last 5 years.² If that rate of growth continues, the hospital's data storage needs will have increased by more than 10,000 times in 21 years' time. While much of the rate of growth will have derived from the retention of previously analogue images in digitised form for the first time, the change is nevertheless massive.

An increasing proportion of the information about us is information about our movements and actions. The sources range from the 'black boxes' recording incidents in our motor cars to the recording of our tollway payments, video images of us going in and out of buildings and moving through public places etc, and of course the continued surveillance of our internet activity and SMS messages.

The further potential for sources of data to fuel this growth is enormous. More and more of the devices around us will be actively networked to the wider world and contain significant processing power – phones, fridges, doorways, internally worn prosthetic devices, all financial transactions etc. Claims have been made that “Analysts envision a time when the system will be used to identify and track every item produced on the planet”.³ Collation of data from these sources adds another dimension – potential tracking of where we are, what we are doing and with whom or what, moment by moment.

For this reason, our 'identity' is one of the most important points of control over personal information. Each of us as individuals is keenly aware that our 'identity' is the 'glue' that holds all this personal information together. For the same reason, organisations either public or private seek information that is connected to an 'identity' because that is often how they add value.

Our 'identity' is a very subtle concept.⁴ Often, it is not necessarily the 'identity' we would assign to ourselves through our lifetime or in any of the myriad roles we occupy, be it any of parent, employee, dance party goer, student, professional society member, seeker of credit or anything else. Sometimes we seek these identities and are likely to be quite happy or even flattered by them. At other times, they are identities

² “Hospital Tackles Data Growth”, Enterprisestorageforum.com, 10 June 2005, online at: www.enterprisestorageforum.com/continuity/features/article.php/3511906

³ “RFID: Tracking everything, everywhere”, Katherine Albrecht, Founder of CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), 2002, online at: www.nocards.org/AutoID/overview.shtml

⁴ This subtlety is explored further in “Proof of ID required? Getting Identity Management Right”, by Malcolm Crompton when Privacy Commissioner, March 2004 – in [HTML](#), [PDF](#) or [Word](#) – online at: www.privacy.gov.au/publications/index.html#S

with characteristics assigned to us by a person or organisation that has been gathering and analysing personal information believed to be related to that identity, while we often have only a dim understanding that it is either happening or what it means, such as our credit rating.

Indeed, it is important to distinguish between an ‘identity’ that has been assigned to us and the ‘profile’ developed about that identity using the information linked (rightly or wrongly) to the identity. ‘Identity’ seeks to define the physical you and me. That identity then is used to seek links between the various elements of our personal histories that have been recorded in order to build a profile. The history includes our behaviours and events in which we have participated.

Moreover, either because of the lack of more subtle thinking or because organisations are actively seeking more information about us, identity is used to authorise or collate activity when it is not inherently necessary, even when the technologies exist to avoid such surveillance.⁵

Fraudsters have become good at making identities fuzzy. They use those fuzzy identities to participate in events that then link in an inaccurate way to the individual who really is that identity. Data then leads to false information, false knowledge and false wisdom.

As such, identity management is arguably the privacy issue of the moment.

In addition, all this information is accessible to a staggering number of ISP, administrator, commercial and other interests in circumstances that range from being covered by very tight legal constraints through the barely legal to the clearly illegal.

Our personal information is being used and re-used ever more imaginatively

Personal information about us now seamlessly moves around the world through back up servers, “24x7, follow the sun” service facilities such as call centres, service bureaus, round the clock problem solving etc.⁶

There are strong legal and commercial drivers as well as developments in information management technologies behind the growth in the use of personal information.

Know your Client requirements, for example, are already embedded in the nation’s Financial Services Reform legislation.

⁵ See, for example: “Proof of ID required? Getting Identity Management Right” (ibid); and “ID Cards - UK’s high tech scheme is high risk”, London School of Economics News Release, 27 June 2005 and from there, link to the LSE Report titled *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

⁶ Google returned over 6 million hits on the search term *24 by 7 follow the sun service* in August 2005. See: www.google.com.au/search?hl=en&q=24+by+7+follow+the+sun+service

Governments have committed themselves to combating money laundering with consequent impact on the detail of our financial transactions that must be collected and analysed. Australia, for example, has been a player in the Anti-Money Laundering campaign for many years, with the *Financial Transaction Reports Act 1988* a major milestone. The Australian Government remains committed to this leadership role and has strongly committed⁷ to implementing the recommendations of the Financial Action Task Force (FATF)⁸ and the Basel II accord.⁹ When implemented, the Anti-Money Laundering initiatives and moves to manage fraud losses will result in a lot more collection and use of personal information. The UK has spelt out its approach in the 2003 Money Laundering Regulations and other initiatives¹⁰

Anti-terrorism initiatives have also strongly focused on gathering, linking and analysing personal information, with travel and immigration information of particular popular interest. Some of these have caused vigorous debate along the way, for example the secret collection of data from airlines to test improved intelligence systems.¹¹

Customer Relationship Management seeks to improve the customer experience, also by much more thorough collection and collation of personal information. As such, it has a lot in common with the collection and uses of personal financial information sought for other purposes such as anti-money laundering and fraud control. Would we expect personal information collected to meet various legal requirements under anti-money laundering and anti-terrorism laws to be used also for CRM without permission?

There is a particularly good case for much wider collection of health information and linkage of the various data sets. Professor Fiona Stanley, Australian of the Year in 2003, makes the case passionately and backs it up with very solid facts to show the real gains it has given society. For example, we have achieved a significant reduction in spinal defects such as spina bifida because of the linkage discovered between folate intake during pregnancy and spinal defects. She attributes this and many other successes to collection and data matching of disparate health data sets.¹² But when

⁷ Being led by the Attorney-General and the Minister for Justice and Customs; see www.ag.gov.au/aml

⁸ The Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989; see www.fatf-gafi.org

⁹ The Basel Committee was established by the central-bank Governors of the Group of Ten countries at the end of 1974. Their Basel II Accord released in 2004 has set out a new capital adequacy framework commonly known as Basel II; see www.bis.org/bcbs/index.htm

¹⁰ See for example “Money Laundering Regulation: Basic Guides and Main Publications”, published by HM Revenue and Customs, online at http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageExcise_InfoGuides&columns=1&id=MONEYSERVICEBUS

¹¹ The JetBlue incident is the most well known. The class action case against it was dismissed in early August 2005, but not before the airline had admitted it had done the wrong thing. See “Judge dismisses privacy suit against JetBlue”, MSNBC/AP, 2 August 2005 at: www.msnbc.msn.com/id/8796381/

¹² Her address to open the 25th International Conference of Data Protection and Privacy Commissioners in 2003 in Sydney was a most comprehensive exposition of the case, online at: www.privacyconference2003.org/speakers.asp#fiona

does excessive collection and use of health information become an invasion of privacy? This was a major theme running through the world renowned report into genetics and privacy by the Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia*.¹³ Much of this work was presaged by the work of the Human Genetics Commission in the United Kingdom¹⁴ and key recommendations in the ALRC report are based on the establishment and work of the HGC.

There is also a strong case for workplace surveillance in particular circumstances, but in all circumstances and of all kinds? Few of us would want to fly on a plane with a pilot under the influence of alcohol or any other drug but what about daily, after lunch alcohol testing for an office job? New South Wales has passed legislation to regulate workplace surveillance.¹⁵ The Victorian Law Reform Commission is conducting an inquiry into such issues and its report is expected to be tabled before the end of the year.¹⁶

In all the circumstances, what has happened to ‘the right to be let alone’?¹⁷ Or is it simply that in the words of Scott McNealy, CEO of Sun Microsystems, “You have zero privacy anyway”.¹⁸

Our personal information is also being abused – lost and stolen

Regardless of whether we think these developments are all for the good, inherently pernicious or somewhere in between, how does our answer change when we learn of the growing impact of identity theft and the appallingly bad records of some data aggregators and others regarding the levels of security protections that they apply to the data they hold?

While there is a wide divergence of statistics, it is clear that ‘something is happening’. *The Bulletin* described this in graphic detail in “Grand Theft Identity” in June 2005.¹⁹ The Sirca report Identity Fraud in Australia completed in 2003 estimated that \$1.1 billion had been stolen this way in Australia in 2001-02. Other reports have

¹³ “Essentially Yours: The Protection of Human Genetic Information in Australia”, ALRC 96, released 29 May 2003 and online via: www.alrc.gov.au/media/2003/index.htm

¹⁴ www.hgc.gov.uk

¹⁵ Summarised in an article titled “Workplace Surveillance Act passed in New South Wales”, FindLaw Australia, July 2005, online at: www.findlaw.com.au/article/13598.htm

¹⁶ Background and terms of reference to the Victorian Law Reform Commission privacy inquiry are at: www.lawreform.vic.gov.au/CA256A25002C7735/OrigDoc/~0456DDC1026247E4CA256A7900217AA4?OpenDocument&1=30-Current+projects~&2=30-Privacy~&3=~

¹⁷ In 1890, in what is now regarded as the first key modern writing on privacy, Warren and Brandeis popularised Judge Cooley’s suggestion that privacy is the ‘right to be let alone’; see Samuel Warren and Louis Brandeis, 1890, ‘The Right to Privacy’, 4 Harvard Law Review 193, 1890, and online at www.louisville.edu/library/law/brandeis/privacy.html

¹⁸ “Sun on Privacy: ‘Get Over It’”, Wired News, 26 January 1999, online at: <http://wired-vig.wired.com/news/politics/0,1283,17538,00.html>

¹⁹ “Grand Theft Identity”, *The Bulletin*, 29 June 2005 <http://bulletin.ninemsn.com.au/bulletin/site/articleIDs/75B9EA5BEE88756DCA25702D0000F426?open&ui=dom&template=domPrint>

suggested that the rate of growth has been overstated, including reputable industry analysis.²⁰

In some circles, ChoicePoint, LexisNexis, Bank America and other US banks, and CardSystems have become household names for the way in which personal information was stolen from them. Some made particular names for themselves by below par responses to consumer concerns when they were found out.²¹

Regardless of the precise figures though, the nature of the threat does appear to be increasing. Misuse of personal information is no longer just a matter of unwanted marketing or delayed credit. Sloppy security has costs for the individual all the way up to society as a whole. There is a professional black market for personal data.²² While stealing data is a security issue, the misuse by bad guys is a privacy issue. One can no longer silo these fields.

What do we think about it?

The general public is becoming aware of these developments and evidence is emerging of the economic damage it is causing through direct losses to individuals and institutions as well as the indirect losses through reduced participation in the online economy etc.

The Office of the Privacy Commissioner in Australia conducted surveys in 2001 and 2004 that give some indication of the impact on public trust among Australians.²³

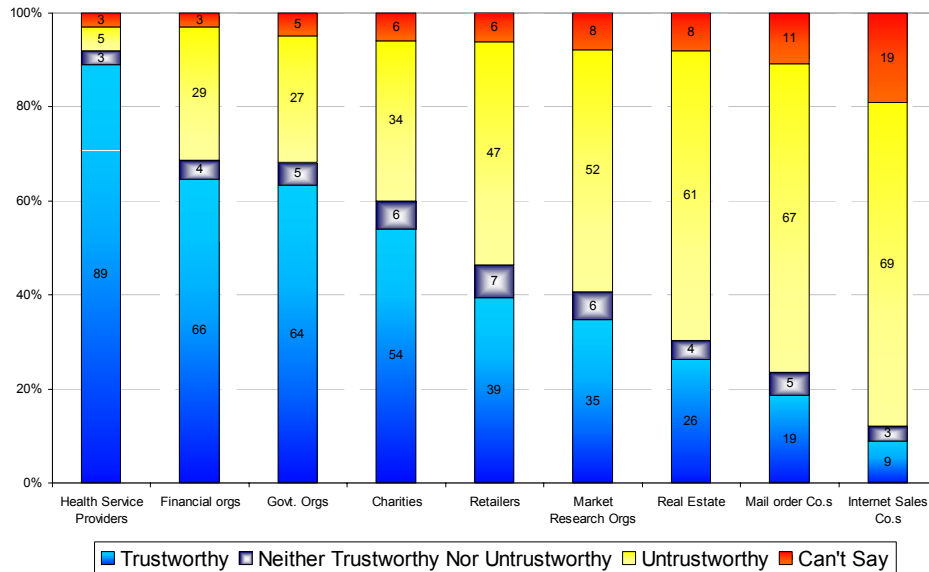
For example, Australians think internet sales companies are rock bottom as untrustworthy, although this probably needs to be disaggregated between companies with a historical and real world reputation, such as the established travel companies, the banks etc compared with those that started as online operations.

²⁰ See for example, “A Primer on Information Security” prepared by The Center for Information Policy Leadership in the law firm Hunton and Williams, August 2005; advance copy available from Malcolm Crompton.

²¹ “Swindle: ‘Somebody Has Got to Pay’”, Internet News, 17 May 2005, online at: www.internetnews.com/security/print.php/3505826; and “The Five Most Shocking Things About the ChoicePoint Debacle”, CSO magazine, May 2005, at: www.csoonline.com/read/050105/choicepoint.html

²² “Phishing economics reveals collectors and cashers”, iTnews.com.au, 1 Aug 2005, online at: www.itnews.com.au/print.aspx?CIID=23899&SIID=35

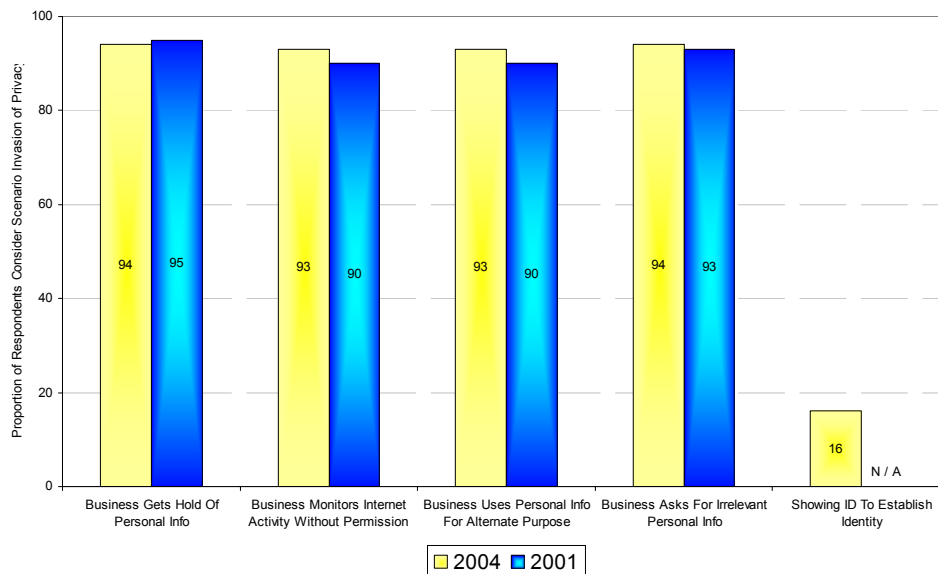
²³ Both surveys are available online at “Research into privacy attitudes in Australia”, www.privacy.gov.au/business/research/index.html



2004 Survey, Figure 12: Respondents' Trust in Organisations

Would you say these types of organisations are trustworthy or untrustworthy when it comes to the protection or use of your personal information?

Moreover, the passage of time has not dimmed the view held by Australians that certain acts and practices are an invasion of privacy, as indicated in Figure 15 of the 2004 Survey.



2004 Survey, Figure 15: Respondents' Perceptions of Invasion of Privacy

Would you say this was an invasion of the privacy of your personal information?

The results shown in Figure 15 of the 2004 Survey are even more significant because the first survey was carried out in mid-2001, some months before the 11 September terror attacks, while the second was carried out some time later in mid-2004. Such evidence does not support the view that Australians now are more prepared to

compromise their privacy than they were before, at least when the only thing at stake is commercial gain.

By contrast, though, these results indicate a contrasting lack of concern about ‘showing ID to establish identity’.

The Information Commissioner’s “Annual Track Research Findings: Individuals” indicate lower, but still considerable concern among individuals in the UK. For example, 83 percent of those surveyed rated “Passing or selling information on to other organisations without your permission” at an 8 out of 10 level of concern, while 78 percent rated “Using information for purposes other than that for which it was intended” at an 8 out of 10 level. More than half of those surveyed rated all government organisations as rating 4 out of 5 for concern over “How confident are you that each of the following handles information appropriately”, with this dropping to a third or less for all non-government organisations.²⁴

Understanding our attitudes on matters such as these nevertheless remains difficult and subtle. For example, a recent survey by the Australian Government Information Office concluded that “Privacy issues have been an area of intense focus in e-government planning. Governments have approached this area sensitively to ensure that citizens retain trust in the Internet as a communication channel and for delivery of government services. However, the survey revealed that concerns about personal privacy were a minor barrier to e-government use.” On the other hand, when it comes to identity issues, the survey also noted the desire to be able to interact with government anonymously and the steps that individuals took as a result, for example making contact by phone instead of online.²⁵

In the US, the respected Pew Internet and American Life project conducted a survey on spyware and reached the top line conclusion that “Nine out of ten internet users say they have adjusted their online behavior out of fear of falling victim to software intrusions”.²⁶

The Ponemon Institute is building quite a repertoire of surveys that demonstrate the link between an organisation’s respect for privacy, its impact on trust in the organisation and from there, its impact on the commercial bottom line.²⁷ More surveys seem to come out on a weekly basis showing the impact of reduced confidence by consumers in online channels. While much of this is US based, the rest

²⁴ “Annual Track Research Findings: Individuals:2004”, Conducted by Quæstor on Behalf of the Information Commissioner’s Office, available online at: www.informationcommissioner.gov.uk/cms/DocumentUploads/Annual%20Track%20Research%20Findings%20Individuals.pdf

²⁵ “Australians’ use of and satisfaction with e-Government services”, Australian Government Management Information Office, 20 June 2005, online at: www.agimo.gov.au/publications/2005/june/e-government_services

²⁶ “Spyware – The threat of unwanted software programs is changing the way people use the internet”, Pew Internet and American Life project, 6 July 2005, online at: www.pewinternet.org/PPF/r/160/report_display.asp

²⁷ See for example “If You Want to Reach Consumers, Think Privacy and Trust”, Darwin magazine, Ethics & Privacy column by Larry Ponemon, Sep 2004, online at: www.darwinmag.com/read/feature/column.html?ArticleId=1171

of us should see this as a foretaste of the future for our own economies if loose data governance also provides sustained evidence of poor performance by those who handle personal information.²⁸

There seems to be particular sensitivity and lack of trust in strong identity management arrangements when they extend beyond small pools of trust (eg between a bank and its customers or an employer and its staff). The extremely poor record of the Social Security number in the US has a lot to answer for this. It is probably making the Real ID Act much less acceptable than it otherwise would be in its effort to standardise driving licences in the US.²⁹ The French government has just abandoned plans to introduce a more robust electronic ID card³⁰, as has the government of Taiwan.³¹ The ID card proposals by the UK government have also been dogged by controversy for similar reasons.³² The recent media debate over the possibility of an identity card in Australia would suggest that the issue remains controversial here, too.³³

The ‘Rules of the Game’ as they are today

Most laws aimed at the protection of personal information are based on regulating various stages of an ‘information life cycle’. The conventions that form the basis of data protection law have been designed to deal with discrete collections of data and discrete histories. They were based on the concept of transparency and individual control (albeit with increasing numbers of exceptions).

²⁸ A short, very recent sample includes:

“Consumers Still Don’t Trust the Internet”, iMedia Connection, 14 Nov 2005, online at: www.imediaconnection.com/global/5728.asp?ref=http://www.imediaconnection.com/content/7275.asp

“Report: ID Theft Haunting Bank Customers”, Internet News, 11 Nov 2005, online at: www.internetnews.com/stats/print.php/3563566

“Web Users Increasingly Wary”, MediaPost Publications, 27 Oct 2005, online at: http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=35558

“Bad-news data letters push consumers to stray”, MSNBC, 4 Oct 2005, online at: www.msnbc.msn.com/id/9581522/displaymode/1098

“Hacking fears bog down online banking growth”, New York Times, 6 Sep 2005, online at: www.nytimes.com/cnet/CNET_2100-1038_3-5851061.html

²⁹ See for example “New plans are in store for an old number”, The Christian Science Monitor, www.csmonitor.com, 10 August 2005, online at www.csmonitor.com/2005/0810/p12s03-ussc.html

³⁰ “Launch of French e-ID card could be postponed”, eGovernment News, 20 July 2005, online at: www.europa.eu.int/idabc/en/document/4476/194

³¹ “Taiwan Constitutional Court places fingerprinting plan on hold”, Privacy International, 22 June 2005, online at: www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-249615

³² “ID Cards – UK’s high tech scheme is high risk”, London School of Economics News Release, 27 June 2005, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

On a lighter note, see “the very model of a modern labour minister : a tribute to charles clarke and his id cards”, eclectictech, at: <http://eclectech.co.uk/clarkeidcards.php>.

³³ See for example “Identity card not part of war on terror”, Editorial, *The Courier Mail*, 19 July 2005, online at: www.couriermail.news.com.au/common/story_page/0,5936,15971974%255E13360,00.html

The quintessential framework was promulgated by the OECD in 1980; one of the most recent is the APEC privacy framework, adopted in November 2004.³⁴

Thus they usually provide that an organisation should:

- give notice to the person about whom it is collecting personal information, or even obtain consent to do so
- only collect the minimum information necessary to carry out its functions or provide the service involved
- identify the primary purpose of collection and limit its uses and disclosures of the personal information to that primary purpose or related purposes
- keep the information secure, complete, accurate and up to date, sometimes being required to subject itself to compliance audits
- allow individuals to see all the information held about them and obtain correction of errors and sometimes be able to require deletion of unwanted information
- deidentify or destroy personal information no longer in use

Privacy is also protected, of course, by a myriad of other laws, including anti-spam law, broader consumer protection law, telecommunications and postal legislation, administrative law such as Freedom of Information and Ombudsmen etc.

Are current protections in privacy law, other consumer protection law and new technologies keeping up? Or are they just falling behind ever further?

The recent report by the Privacy Commissioner on the operation of the private sector provisions of the Privacy Act 1988 found that there was that there is “no fundamental flaw” with the private sector provisions in the Privacy Act.³⁵ However, in Recommendation 69 of the report, she also recommended that “The Australian Government should consider ... reviewing the National Privacy Principles and the definition of personal information to assess whether they remain relevant in the light of technological developments since the OECD principles were developed”.

Professor Fred H Cate, a leading US academic and public commentator on information law in digital networks certainly considers that change is needed. He recently remarked that “The greatest failure of FIPPS [Fair Information Practice Principles] as applied today is the substitution of maximizing consumer choice for the original goal of protecting privacy while permitting data flows. As a result, the energy of data processors, legislators, and enforcement authorities has been squandered on notices and often meaningless consent opportunities, rather than on enhancing privacy. Compliance with data protection laws is increasingly focused on

³⁴ “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, adopted by OECD member countries on 23 September 1980, online at: www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html; and “APEC Ministers Endorse the APEC Privacy Framework”, Media Release from Asia-Pacific Economic Cooperation, 20 Nov 2004 with links to the Framework itself, online at www.apec.org/apec/news_media/media_releases/201104_apecminsendorseprivacyfrmwk.html

³⁵ “Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*”, undertaken by the Privacy Commissioner of Australia, released on 18 May 1988 and online at: www.privacy.gov.au/act/review/index.html

providing required notices in proper form and at the right time, rather than on ensuring that personal information is protected.”³⁶

One area that probably bears more analysis is the economic distribution of the benefits and costs of the trade in personal information. Is the current distribution between the parties appropriate or are there significant asymmetries between the understanding of organisations and the wider population of the value of personal information? Are there large ‘capacity to trade’ gaps, arising for example out of increasing returns to scale on data as it is aggregated favouring large aggregators over the individual?

Where does this all leave us?

The major points from the discussion so far can be summarised as follows:

- The data revolution has changed our world, possibly for ever. Traditional privacy regulatory frameworks have been based on the concept of transparency and individual control. The intention behind them was to give effect via individual control through notice, consent and limitations on collections and use. However, have we reached the point where we need to manage inappropriate effects more directly?
- What are the benefits and costs of the burgeoning collection, use and disclosure of so much personal information and just as importantly, how are they distributed – who benefits and who pays?
- Have we got the right balance between identity, anonymity and the public interest?
- Related to the previous point, has the increasing collection of personal information, its circulation and re-use provided a much stronger incentive for criminal intrusion than ever before?

Is there a better way? Questions for the future

This begs the question of what it means to have a ‘better way’ and that it is based on perceived problems with the present arrangements and anticipated future developments.

This question is going to be quite controversial and is one that seminar participants may well want to discuss in some detail.

To foster discussion, the following are some of the possibilities that might be explored.

Is it a matter of law?

Drawing on Fred Cate’s analysis, are current privacy protection laws too ‘front end loaded’ by being too dependent on notice, collection limitation and purpose limitation? Is there something to be said for emphasising ‘back end’ frameworks,

³⁶ From a draft manuscript for a forthcoming book. Quoted with the author’s permission.

based around a security, data quality and general information governance framework that is well enforced? Perhaps the solution is strong framework of audit, continuous disclosure and clear civil and criminal penalties. After all, this is the framework that already applies to the governance of another category of vital information held in an organisation, namely financial information. Have we reached a point where a similar framework ought to apply to personal information held in the organisation?

More particularly, can the law redress any imbalances by internalising risks of failure and misuse to the organisation through such combinations as requiring greater transparency, regular published audit in a complete information governance framework, allocation of a greater proportion of risks of failure to the organisation including through private class action?

Other papers to be presented to the seminar will also raise specific proposals for strengthening the legislative framework, for example powers imposing stronger audit powers, stronger information collection powers, injunctive relief, and stronger sanctions.

Evidence indicates that the transparency created by such processes could have powerful impact. However, by themselves are they enough? A recent change to the law in California requires an organisation to notify individuals if it believes that something has gone wrong with the personal information it holds. This law is credited with much of the exposure over recent months of just how lax information security is at present in a number of firms in the US and there is no doubt that it is costing them dearly. This could be a key way of ensuring that compliance is not just externally driven through external audit impositions and responding to complaints but also internally driven by the impact of customer response to widely publicised disclosures of failure.

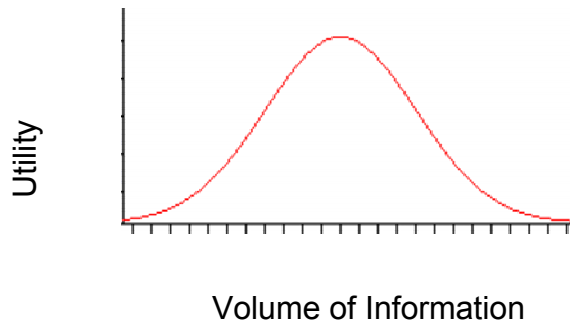
On the other hand, the online economy is still proving hard to regulate effectively. The stand out example is spam. Despite the existence of anti-spam legislation in many nations and some vigorous court action, spam remains a serious problem.

In short and most importantly, any proposals to strengthen data protection law will need to be able to demonstrate

- the need for doing so;
- that they are effective;
- that they are the least cost from a regulatory burden perspective; and
- that as far as possible, they are self-administering because the incentive to respect personal information is internalised not just externally imposed.

Is ‘more information always better information’?

Is there in fact an optimum of some sort? Instead of the usual assumption that ‘more is better’, is the utility of information, including personal information, more like a bell shaped curve of some sort, such as the following?



If so, do we let the market place discover the optimum? Does the market place need some ‘help’ to do this by being better informed in some way? Traditional collection limitation rules in privacy law seem to have had limited effect, so is there an alternative?

Do we just need a better way of analysing and managing it all?

There is the adage that data well managed leads to information; information understood well leads to knowledge; information with insight can lead to wisdom:

Data → Information → Knowledge → Wisdom

Just as Windows made DOS much easier to use, is a technological solution possible? Is it possible to construct an equivalent ‘Windows for Privacy’?

An ambitious joint Canadian / EU research project has attempted just this. The Privacy Incorporate Software Agent (PISA) project aimed at building a “privacy guardian for the electronic age by:

- Demonstrating Privacy Enhancing Technology (PET) as a secure technical solution to protect the privacy of the citizen when he/she is using Intelligent Agents (called shopbots, buybots, pricebots or just “bots”, a short for robot) in E-commerce or M-commerce applications, according to EC-Directives on Privacy.
- Interacting with industry and government to launch new privacy protected services.
- Proposing a new open standard for Privacy Protected Agent Transactions to Standardisation Bodies.”³⁷

Alternatively or in combination with such developments, is it possible to build simple to read ‘safety meters’ to improve individual judgement?

³⁷ The project, including a most comprehensive “Handbook of Privacy and Privacy-Enhancing Technologies, the case of Intelligent Software Agents” is online at: www.pet-pisa.nl. For an interesting critique, see “Protecting privacy in software agents: Lessons from the PISA project”, Patrick, A.S., a presentation at the DIMACS Workshop on Usable Privacy and Security Software, 7-8 July 2004, Piscataway, NJ, USA, online at www.andrewpatrick.ca/pisa/LessonsFromPISA.pdf

Are human agents of some sort the answer?

The results of the PISA project appear to have had limited impact in the wider world to date. Is it possible to establish an organisation or person who can act genuinely as our agent? Would it be possible for such an agent to handle all the consents we have given, for example?

The human agent approach has indeed been attempted. A well known example is the system of Caldicott Guardians established by the UK National Health Service. Caldicott Guardians “are senior staff in the NHS and social services appointed to protect patient information”.³⁸

In the commercial world, though, is it possible to construct some sort of equivalent that pays for itself or is it inherently a very uneconomic approach? Is it possible to ensure that such an agent is genuinely acting in our own interests?

Privacy respecting identity management

This concept has now become respected, mainstream thinking. Very recent thinking in identity management technologies is beginning to describe the characteristics of good identity management and how it might be delivered. In particular, Microsoft published its Laws of Identity in May 2005.³⁹ The laws state the following:

1. “User Control and Consent – Technical identity systems must only reveal information identifying a user with the user’s consent.
2. “Minimal Disclosure for a Constrained Use – The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.
3. “Justifiable Parties – Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. “Directed Identity – A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. “Pluralism of Operators and Technologies – A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6. “Human Integration – The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
7. “Consistent Experience Across Contexts – The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

³⁸ “NHS Caldicott Guardians”, available on the UK National Health Service at: www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT_ID=4100563&chk=ZdxTGp

³⁹ “The Laws of Identity”, Kim Cameron, Identity and Access Architect, Microsoft Corporation, May 2005 and online at: <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/lawsidentity.asp>

The London School of Economics proposals previously mentioned also put forward similar concepts⁴⁰, as I did in 2004 as Privacy Commissioner.⁴¹ The Privacy and Identity Management Project for Europe (PRIME) is also aiming at very similar objectives in a very ambitious project funded at more than \$10 million.⁴² None of these proposals are exactly the same, but they do respond to the call to produce something better than the oft-espoused approach of ‘one number per person to be used in all circumstances’ that security specialists have shown is deeply flawed even from a security perspective.⁴³

What about other Privacy Enhancing Technologies (PETs)?

Besides better identity management, are there other ways of respecting our privacy while taking advantage of the full potential of new technologies? A landmark paper that asked this question and popularised the concept of PETs was written by the data protection authorities of the Netherlands and the Province of Ontario in Canada.⁴⁴

Anonymous, or pseudonymous, actions are one good example. IBM has developed idemix, an anonymous credential for e-transactions.⁴⁵ A remarkable recent development is a privacy enhanced RFID chip that can operate in a number of modes, including “Privacy Mode”, where “the RFID tag is under complete Owner control and does not respond to non-approved requests”, without leaking information even when responding to authorised requests.⁴⁶

Or is there no magic bullet solution?

Is any ‘better way’ in fact a combination of improved public understanding of the issues, different laws, better technologies, stronger governance structures supported by real accountability and powerful error correction and other restitution measures? It has taken all of these tools and more to address the road toll over a generation.

Regardless of the answers, most of us would agree that we are seeking to lead dignified private lives in which we respect individuals and the personal information about them, while being take advantage of the wonderful new technologies and services already around us and emerging in the future. I am sure we can do it.

⁴⁰ “ID Cards - UK’s high tech scheme is high risk”, London School of Economics News Release, 27 June 2005 and from there, link to the LSE Report titled *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

⁴¹ “Proof of ID required? Getting Identity Management Right”, Office of the Privacy Commissioner, March 2004, online at www.privacy.gov.au/news/speeches/sp1_04p.pdf

⁴² PRIME research papers are available online at: www.prime-project.eu.org/public/prime_products/deliverables/

⁴³ Bruce Schneier has written extensively on this question. He published an easy to read summary of the arguments in “National ID will make US less secure”, *The Sydney Morning Herald*, 19 April 2004, online at: www.smh.com.au/articles/2004/04/19/1082326122398.html

⁴⁴ “Privacy-Enhancing Technologies: The Path to Anonymity”, Information and Privacy Commissioner/Ontario Canada and the Registratiekamer, The Netherlands, August 1995, online at: www.ipc.on.ca/scripts/index.asp?action=31&P_ID=11361&N_ID=1&PT_ID=11351

⁴⁵ “idemix: pseudonymity for e-transactions”, IBM Zurich Research Laboratory, online at: www.zurich.ibm.com/security/idemix/index.html

⁴⁶ “RFIDSec - When security means business!”, www.rfidsec.com