INFORMATION
INTEGRITY
SOLUTIONS

Respecting people, their individuality and their personal information

A Position Statement for:

W3C Workshop on
Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement

Malcolm Crompton

Managing Director, Information Integrity Solutions Pty Ltd
Privacy Commissioner of Australia, 1999 – 2004
www.iispartners.com

Ispra, Italy
September 2006

The protection of personal information – Is there a better way than traditional data protection law?

Such a question begs others, such as: "what do we mean by a 'better way'" and "what are the problems with the present arrangements and can they handle the future".

This is a question for a bigger paper. For some background thinking, though, see "Respecting people, their individuality and their personal information: The Key to Connected Government, now and in the future", presented to the Public Services Summit in Stockholm in December 2005.[1]

Is it a matter of law?

Drawing on analysis by Fred Cate, Distinguished Professor and Director, Center for Applied Cybersecurity Research at Indiana University, 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, 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?

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 invitation 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.

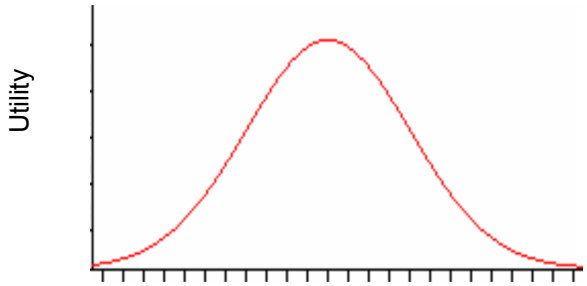
In short and most importantly, any proposals to strengthen data protection law will need to be able to demonstrate

- 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.

[1] Online at: www.cisco.com/web/learning/le21/le34/nobel/2005/post/presentations.html or www.iispartners.com/publications.html

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?



Volume of Information

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."[2]

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

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?

[2] 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

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".[3]

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.[4] 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.

The London School of Economics proposals previously mentioned also put forward similar concepts[5], as I did in 2004 as Privacy Commissioner.[6] 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.[7] 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.[8]

---

[3] "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

[4] "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/lawsofidentity.asp

[5] "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] "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

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

[8] 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

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.[9]

Anonymous, or pseudonymous, actions are one good example. IBM has developed idemix, an anonymous credential for e-transactions.[10] 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.[11]

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.

Conclusion

Treating consumers and citizens without respect is a short term strategy. World wide, the market is responding against organisations public or private that do not respect the personal information about consumers is likely to continue. Even if the change in this direction is slow in a particular economy, poor privacy protection of personal information may inhibit that economy from offering outsourced data processing services.

The best approach to designing products and services is to work within a recognised Privacy Framework such as the APEC Privacy Framework[12] and consider:

- Security and Privacy – working together
- Built in is better than built on
- Identity Management is the key to privacy
- Look at the law
- There is extra work for an organisation that expects to export or obtain services overseas
- Privacy Impact Assessments work in your favour
- Start somewhere easy, for example with Multi-Layered Privacy Notices.[13]

---

[9] "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

[10] "idemix: pseudonymity for e-transactions", IBM Zurich Research Laboratory, online at: www.zurich.ibm.com/security/idemix/index.html

[11] "RFIDSec - When security means business!", www.rfidsec.com

[12] Online at: www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[13] This concept has been endorsed very widely by privacy regulators, including a full meeting of data protection commissioners globally in 2003 (www.privacyconference2003.org/resolution.asp) and more recently in more detail by the Article 29 Committee of European data protection supervisors in Opinion WP 100 adopted on 25 November 2004 (www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm)