Commissioner for Privacy and Data Protection

Background paper

Privacy by Design:
Effective Privacy Management in the Victorian public sector

The Commissioner for Privacy and Data Protection (CPDP) has formally adopted 'Privacy by Design' (PbD) as a core policy to underpin information privacy management in the Victorian public sector.

This background paper provides information and context about PbD, an account of its main features and explains how and why PbD is helpful for the community and for Victorian public sector organisations.

Introduction

PbD is a specific approach to privacy, developed by the former Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian,[1] initially in the 1990s but continuing over the subsequent decades. The privacybydesign.ca website that she created provides a rich archive of PbD material and initiatives, many of them relevant to the Victorian public sector. This background paper has been adapted from that material, in particular Dr Cavoukian's description of the seven foundational PbD principles. Dr Cavoukian's agreement to permit her materials to be included in this background paper is gratefully acknowledged.

What is Privacy by Design?

PbD is a methodology that enables privacy to be 'built in' to the design and architecture of information systems, business processes and networked infrastructure. PbD aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information. It involves a level of intentionality regarding privacy management that marks a genuine departure from more common, well meaning but ad hoc approaches to privacy.

PbD enables public sector policy-makers, information technology professionals and those responsible for delivering services to the community to approach privacy as a 'design feature' of public sector processes and activities rather than as a compliance burden to be endured or to which lip-service is given. It shifts the privacy focus to prevention rather than compliance, using innovative approaches that are anchored in genuine respect for individuals' personal information.

In doing so, PbD lays the ground rules for changes to the way that public sector information-based initiatives are currently designed, managed and implemented. Victorian regulators have consistently highlighted poor leadership, planning and project management as being some of the causes of failures to deliver information-based projects on time, within budget and having full functionality. They have also noted that the gateway process – which is designed to provide independent advice and oversight to those who manage high value, high-risk projects – has not always functioned effectively.

By focusing on the design and operation of information systems throughout their lifecycle, PbD supports efforts to address these problems. For example, better privacy means that costly privacy retrofitting will not be required, generating significant cost savings. PbD forces leaders and project managers to direct their attention to the policy and operational objectives information projects are intended to achieve in a way that respects privacy – if the project does not meet legal requirements, it needs to be rethought so that it does. Equally, if a project cannot demonstrate that it complies with privacy or other regulatory requirements the gateway process should identify this and require remediation. As such, PbD constitutes a basis for cultural change in the way that the Victorian public sector plans, develops and implements information projects.

Based around seven 'foundational principles', PbD rejects claims that privacy and the adoption of new ICT such as Web 2.0 technologies are mutually exclusive. Such arguments have been used misleadingly to justify claims that

1 Dr Cavoukian is currently Executive Director, Institute for Privacy and Big Data, Ryerson University, Toronto, Canada

privacy impedes innovation, prevents public institutions from using better technology to provide more efficient and effective services for the community and dictate that privacy most often becomes the loser of a zero-sum game.

Our decision to adopt PbD reflects the opportunity we have as the new office overseeing Victoria's *Privacy and Data Protection Act 2014*, to drive cultural change and to promote more meaningful and contemporary approaches to information privacy in Victoria.

Our adoption of PbD links privacy in Victoria to broader international privacy developments, such as:

- The International Conference of Data Protection and Privacy Commissioners unanimously endorsed PbD in 2010. Their resolution recognises PbD as an 'essential component of fundamental privacy protection' – and urges its adoption in global privacy regulation.[2]
- In the USA, The Federal Trade Commission's (FTC) 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*,[3] proposed a framework for business and policymakers with PbD as a core value and its adoption featured as one of three key recommendations.
- In 2014, the European Commission announced that:

  'Privacy by Design' and 'privacy by default' will become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks.[4]
- In the UK, the Information Commissioner's Office has stated that:

  Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

  — Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

  — Increased awareness of privacy and data protection across an organisation.

  — Organisations are more likely to meet their legal obligations and less likely to breach the *Data Protection Act*.

  — Actions are less likely to be privacy intrusive and have a negative impact on individuals.[5]

[2] http://www.justice.gov.il/PrivacyGenerations/adopted.htm

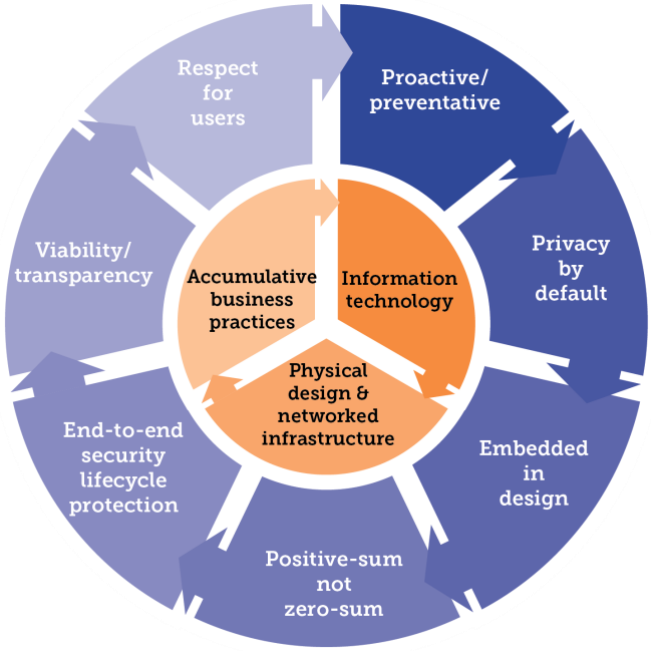
[3] http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

[4] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

[5] http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design

The seven foundational principles

PbD is based on 7 foundational principles:



1. Proactive not reactive, preventative not remedial

PbD is characterised by proactive rather than reactive measures. It anticipates and works to prevent privacy invasive events occurring in the first place. PbD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy breaches once they have occurred – rather, it aims to prevent them from occurring. PbD comes before the fact, not after focusing on prevention. This implies:

- a clear commitment by organisations to set and enforce high standards of privacy
- that this commitment is shared by the individuals working within and across an organisation, in a culture of continuous improvement
- that organisations establish and maintain practices and methods to address poor privacy design, anticipating poor privacy practices and outcomes, and correcting any negative impacts before they occur in proactive, systematic and innovate ways.

2. Privacy as the default setting

PbD seeks to deliver the maximum degree of privacy by ensuring that personal information is automatically protected in any given ICT system, business practice or process. It is not left to an individual to assert her or his privacy in order to obtain it. Even if an individual does nothing, her or his privacy should remain intact. No individual action is required to protect privacy – it is built into the system, by default.

3. Privacy embedded into design

PbD seeks to ensure that privacy is embedded into the design and architecture of information systems, business practices or processes or other initiatives involving the collection and handling of personal information. It is 'built in' intentionally, not 'bolted on' as an afterthought. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is viewed as integral to the system, and delivered without diminishing its functionality. Privacy, good project governance, leadership and project management are inextricably linked.

4. Full functionality: positive-sum, not zero-sum

PbD seeks to accommodate all legitimate interests and objectives in a positive sum "win-win" manner, not through an outmoded zero-sum approach where unnecessary compromises or trade-offs are made. PbD avoids false dichotomies, such as 'privacy versus security', by demonstrating that it is possible to have both.

Privacy is often simplistically characterised as just a 'balancing process' in which privacy is caught up in a 'zero-sum paradigm'. This means that two goals are considered to be mutually exclusive and that each goal can only be attained at the expense of the other: i.e., both values cannot be attained simultaneously. For example, the right to privacy may be 'traded off' to achieve national security goals or for law enforcement purposes. A zero-sum approach to managing competing goals has meant that privacy rights are often inappropriately compromised in favour of achieving other more urgent goals because one side has to 'win' for outcomes to be achieved. It is inappropriate to think that the inevitable result of a balancing process is that there will be winners and losers.

PbD can bring about a paradigm shift in thinking by demonstrating how ICT, introduced to serve one function, can be designed and implemented in a manner such that privacy is maintained or enhanced, without derogating from the functionality of the technology. By building privacy into the design and implementation of information systems, the goal of protecting an individual's privacy and the goal that the system sets out to achieve can be attained simultaneously. PbD shifts the traditional zero-sum paradigm to a positive-sum paradigm, in which both goals are maximised to the greatest possible extent.[6]

5. End–to–end security – full lifecycle protection

PbD, having been embedded into systems and practices before personal information is collected and stored, is able to extend securely throughout the entire lifecycle of the information involved – appropriate security measures are essential to privacy, from start to finish. This ensures that all personal information is kept securely across its lifecycle from collection through to destruction.

6. Visibility and transparency – keep it open

PbD seeks to assure all stakeholders that personal information-based public sector practices and technologies operate according to stated promises and objectives and that these are subject to independent investigation and verification. All of the collection and handling steps along the way are visible and transparent, to users and providers alike.

7. Respect for user privacy – keep it user centric

Above all, PbD requires managers, architects and operators to keep the interests of the individual at the forefront by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options, keeping it user-centric.

All seven foundational principles work together and need to be implemented holistically: PbD can't be 'cherry picked.'

6 Ann Cavoukian and Khaled El Eman, A Positive-Sum Paradigm in Action in the Health Sector, Information and Privacy Commissioner, Toronto, 2011 http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf

The Victorian context

Over a number of years, independent regulators in Victoria have highlighted problems with public sector approaches to managing personal information and security, pinpointing a range of deficits that led to the compromise of the privacy, confidentiality and integrity of personal information collected and handled by the Victorian public sector.

In 2009 the Victorian Auditor-General's (VAGO) report, *Maintaining the Integrity of Personal Information*, examined how personal information was being stored, processed and communicated by the Victorian public sector. The report concluded that 'the confidentiality of personal information collected and used by the public sector can be, and has been, easily compromised.'[7]

At a high level, VAGO attributed its finding to flaws in governance and culture, practice and technology. VAGO found that information governance arrangements had not kept pace with Victoria's increasingly complex and sophisticated information sharing environment. It highlighted challenges such as:

- who 'owns'[8] personal information
- how can recipients provide equivalent standards of privacy and security to shared information
- which party is responsible if personal information is lost, leaked or its confidentiality is otherwise compromised.

VAGO noted 'fundamental flaws' in applying the *Victorian Government Risk Management Framework* and the fact that information security risks were not effectively managed because of disjunctions between operational staff and executive management. In turn, an inadequate information security culture had lead to unauthorised persons having access to personal information, controls such as appropriate logging and audit capabilities were inadequate or not used effectively, there were failures to securely classify personal information and compliance shortfalls were compounded by a lack of effective monitoring.

VAGO followed-up its 2009 report with a report into the *Whole Of Victorian Government Information Security Management Framework* in November 2013. Although the focus of the report was on information security and not broader privacy issues, familiar themes emerged. These included a lack of clarity about the roles and responsibilities of agencies overseeing information security, a lack of guidance for outer-budget agencies and a lack of central oversight, coordination and accountability.

The Victorian Ombudsman has also commented on the problems encountered by the Victorian public sector in an own motion investigation into ICT enabled projects, stating that:

> *The public sector is not managing ICT enabled projects effectively, as demonstrated by the current difficulties that Victoria is facing in this area and the increasing adverse public comment about major ICT enabled projects. A new and more disciplined approach is required if the government is to avoid being faced with continuing cost overruns and failures to deliver.*[9]

Some of the common themes that the Ombudsman identified were:

- lack of leadership, accountability and governance
- poor planning
- poor project management.

Although PbD is not a complete remedy for all of these problems, implemented properly it contributes significantly to the resolution of many of the key issues that have been identified by Victoria's regulators. Implicit in good leadership

7 VAGO, Maintaining the Integrity and Confidentiality of Personal Information, 2009, http://www.audit.vic.gov.au/publications/2009-10/20091125-Data-Integrity-Full-Report.pdf

8 VAGO uses the term 'owns' in a non-legal sense, i.e., as denoting who is responsible for personal information in shared environments

9 Victoria Ombudsman in consultation with the Victorian Auditor-General, Own Motion Investigation into ICT-enabled Projects https://www.ombudsman.vic.gov.au/getattachment/d5e69dd1-400d-42cd-a570-9c6b21c4bb1e>.

and governance is a strategic approach to information-based initiatives that clearly articulates the improvements sought to be achieved. Good project management requires a risk-based approach that delivers on the strategic vision. This includes recognising and working within the applicable policy, business and regulatory environments. PbD contributes to this by placing privacy planning and risk management front and centre in the strategic development, project planning and implementation process.

Victorian regulators have stated that, on average, large ICT-enabled projects will have more than doubled in cost by the time they are finished, that 70% of projects are not delivered on time and that 80-90% fail to meet performance objectives. They have identified 'abject waste' associated with abandoned projects. They have noted that this represents 'many foregone hospital beds, trains, teachers, police, and child protection workers.'[10]

These concerns summarise the overwhelming failure of ICT-enabled projects to produce public value commensurate with the community's investment and expectations.

PbD and public value

Although privacy is conceived of as an individual right, PbD adds an additional community dimension to it by recognising that privacy contributes to the creation of public value.

The theory of public value was developed by a Harvard University-based team led by Professor Mark Moore. Moore argues that 'the task of a public sector manager is to create public value' by expressing citizens' 'collective aspirations through the operations of governmental organisations.'[11] Public value is viewed as the public sector correlative to the familiar private sector concept of shareholder value. It is concerned to establish the combined view of the community about what it regards as valuable.

The OECD gives six broad examples of public value:

- goods and services that satisfy the desires of citizens and clients
- production choices that meet citizen expectations of justice, fairness, efficiency and effectiveness
- properly ordered and productive public institutions that reflect citizens' desires and preferences
- fairness and efficiency of distribution
- legitimate use of resources to accomplish public purposes
- innovation and adaptability to changing preferences and demands.[12]

Almost without exception the production of public value by or for the Victorian public sector depends on business processes and information systems that collect and process data – more often than not, personal information. The OECD argues that as new technologies become embedded in the day-to-day lives of individuals and the activities of the public and private sectors, they shape the community's expectations of government. The challenge is to integrate them into public sector modernisation that respects privacy *and* the production of public value.

PbD aligns with the integrative approach suggested by the OECD by enabling privacy to be embodied in information systems and business processes, not merely as an efficiency measure but to meet community expectations about government's use of personal information and as shaping service delivery. PbD promotes cost savings in ICT enabled projects, supports good governance and project management and provides for the least intrusion into the privacy of individuals.

[10] ibid, pp 4-5

[11] Mark Moore, 'Public Value as the Focus of Strategy', *Australian Journal of Public Administration*, Vol. 53, No. 3, 1994, pp. 296-7

[12] OECD, Recommendation of the Council on Digital Government Strategies, adopted on 15 July 2014, p6

Implementation

Organisations can implement PbD in a number of ways, from a project-by-project approach or a full rollout approach.

Optimally, PbD should be implemented across an entire organisation. However, in practice, implementation may initially occur on a project-by-project basis. In a case study conducted jointly by the Canadian Privacy Commissioner and IBM, it was suggested that it may be wise to 'start small, learn and expand.' A project-by-project approach nevertheless carries the risk that in the long term, a specific process or project may be privacy-protective but the entire organisation may not be. A project-by-project approach should be seen as an interim step to a full rollout of PbD.

Some of the most useful tools that can be used to implement PbD are Privacy Impact Assessments and Security Incident Management.

Privacy Impact Assessment (PIA)

A Privacy Impact Assessment is a point-in-time process that is designed to assist public sector organisations to identify and mitigate privacy risks and to identify and evaluate privacy solutions. It should be used throughout the development and implementation of any project involving the collection and handling of personal information or when making changes to existing systems. A PIA should be regarded as part and parcel of normal project management processes.

Although the *Privacy and Data Protection Act 2014* does not explicitly *require* Victorian public sector organisations to undertake a PIA, most must comply with the *Victorian Risk Management Framework* (VRMF).[13] The VRMF requires public sector organisations 'to actively manage the risks of breaches to a citizens' privacy.'[14]

The VRMF requires public sector organisations to develop their own risk management policies and frameworks which should, amongst other things:

- describe the organisation's understanding of risk in the context of its operations, legislation and strategies
- describe its overall approach, intention and procedures used to identify, analyse, evaluate and treat risks.[15]

The VRMF also emphasises that risks 'need to be managed in the context of achieving organisational goals and objectives. Risk management should be an integrated part of strategic planning, performance management and governance across the public sector.'

A PIA is the appropriate method to address privacy risk within an organisational approach to risk management. Thus, although conducting a PIA is not a mandatory legal requirement, the Commissioner will often ask whether a PIA has been undertaken, and will invariably require a PIA to be undertaken when public sector organisations seek to obtain a Public Interest Determination, seek to establish an Information Usage Arrangement or if Certification is sought.

Our web site contains detailed information about PIAs and how to undertake them. See http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/privacy-impact-assessments-guide/$file/guideline_05_09_no1.pdf.

Security Incident Management

Good security is essential to good privacy: without it, personal information can be easily compromised and, in many cases, security breaches involving personal information are difficult to remediate effectively.

[13] http://www.dtf.vic.gov.au/Publications/Victoria-Economy-publications/Victorian-risk-management-framework-and-insurance-management-policy

[14] Ibid, p22

[15] ibid, p12

IPP4 is the only overarching legally enforceable personal information security obligation imposed on public sector organisations. It requires them to take reasonable steps to secure personal information. One of the key processes that helps this obligation to be met is Security Incident Management (SIM).

SIM assists organisations to manage information security events, incidents or vulnerabilities. It provides for a disciplined and immediate response to security incidents in a manner that protects affected individuals, meets regulators' expectations and ultimately preserves organisational reputation. SIM is a component of broader requirements for organisational information security management. It consists of four key stages:

- **Prepare** – to deal with incidents e.g., prepare an incident management policy and establish a competent team to deal with incidents
- **Detect** – identify and report information security breaches
- **Handle** – assess incidents, decide how to address them, respond to them
- **Prevent** – learn the lessons. This means more than just identifying how things could have been done better – it requires making changes to improve the process.[16]

Privacy by ReDesign

Embedding new privacy practices may be challenging for organisations that are already operating within existing privacy structures and practices. 'Privacy by ReDesign' is an extension of PbD, and offers a solution for organisations to reach the end state that PbD aims to achieve.[17] Privacy by ReDesign maintains the seven foundational principles of PbD, but applies them in new ways.

Privacy by Redesign consists of three 'R's': Rethink, Redesign and Revive:

- **Rethinking** – reviewing an organisation's risk mitigation strategies by looking at how much personal information is collected for a particular purpose and how long it is retained
- **Redesigning** – looking to ways of improving the functioning of an organisation's systems from a privacy perspective, in order to create a positive-sum outcome between privacy protection and achieving organisational objectives
- **Reviving** – reviving its system to encapsulate a privacy-protecting agenda.

Privacy by Redesign is often best approached incrementally, rather than by a complete overhaul of systems and practices all at once. This is because there are a range of factors that can influence organisations' systems and practices, including external forces such as community expectations, internal forces and the cost of redesign. These need be taken into account when organisations Rethink, Redesign, and Revive their privacy strategies and approaches.

Conclusion

PbD enables the Victorian public sector to approach privacy in new and more productive ways that centre on prevention rather than remediation. It means that privacy concerns are identified and mitigated early and comprehensively in an environment where privacy is not the inevitable loser in a zero sum game. The payoff is significant: improved client relationships, better client satisfaction and trust, support for ICT initiatives, cost savings, reduced legal liabilities and more efficient public sector operations. PbD sets the scene for a culture of privacy where privacy is woven into the fabric of day to day organisational practices such that it becomes a part of business as usual activities that sustain and promote public value.

[16] Further guidance on information security incident management can be found at http://www.iso27001security.com/html/27035.html

[17] Ann Cavoukian & Marilyn Prosch, *Privacy by ReDesign: Building a Better Legacy*, Information and Privacy Commissioner, Toronto, 2011, p. 3.