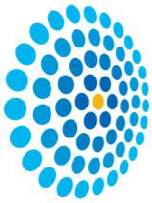


Centre for Information Policy Leadership
Hunton & Williams LLP

The Centre for Information Policy Leadership's Response to the Public Consultation on the Proposed Personal Data Protection Bill

Martin E. Abrams
President
The Centre for Information Policy Leadership
at Hunton & Williams LLP
2200 Pennsylvania Avenue, NW
Washington, DC 20037
E-Mail: mabrams@hunton.com

TABLE OF CONTENTS

Summary of Major Points 3

Comments 4

Limitations of Consent as a Mechanism for Data Protection 5

Making Clear the Scope of the Legislation 6

Conclusion 7

Summary of Major Points

The Centre for Information Policy Leadership's comments will focus on two topics.

1. The Centre will explore the legislation's reliance on consent to protect individuals, and why consent processes place too much burden on individuals and limit organizational flexibility.

2. The Centre will discuss the wording of section 5 on jurisdiction and whether it is achieving the objectives that Singapore identified for this legislation.

The Centre appreciates the opportunity to participate in this consultation.

Comments

The following comments are in response to the consultation on the draft Singapore Personal Data Protection legislation and are prepared by the Centre for Information Policy Leadership. The Centre appreciates the opportunity to participate in this consultation.

The Centre for Information Policy Leadership is a global information policy development organisation situated in Washington, D.C. It was established in May 2001 by leadership companies and Hunton & Williams LLP, and is located within the law firm. The Centre is financially supported by approximately 40 member companies.

The Centre has led or participated in projects and discussions in Asia, Europe, Latin America and North America. It has been active at both APEC and the OECD. The Centre is the secretariat for the Global Accountability Project now in its fourth year. The Centre participated in a forum in Singapore on December 2, 2011 to discuss the next generation of privacy law. The Centre's program includes participants from government, regulatory agencies, NGOs and business. Our mission is to formulate balanced policy responses to the complex privacy and security challenges of an information driven economy.

While these comments have benefited from the insights and review of some member companies, the Centre's views and the views expressed in this response are its own and do not necessarily reflect those of its member companies, the law firm of Hunton & Williams LLP, or the firm's clients.

As stated above, the Centre's mission is information governance that facilitates data driven growth in an information based economy, while still preserving space for individual privacy. Section 3 of the proposed Singapore legislation states this objective well:

> *The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognizes both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.*

The legislation's purpose statement is powerful, but reflects some dated concepts from legacy privacy regimes. Early data protection theory equated individual control with effective protections from the misapplication of personal information. Such an approach was possible when data processing systems performed one and only one application. Furthermore, most of the data was provided directly from the consumer, and was explicitly contributed by the individual in explicit actions rather than having been generated as a byproduct of the individual's interaction with the world.

Gone are the days when individuals on their own or with the aid that comes with legislation could protect their own data. Giving the responsibility to each individual to understand the risks related to modern data applications is too much of a burden to place on them. The matter has now simply become too complex and too abstract. Today the individual needs the organisation

to use information in a responsible and answerable manner. The individual needs policymakers to place that burden on organisations.

Such an approach also enhances the organisation's ability to be entrepreneurial with data. It does so by giving the organisation the initiative in determining how data protection principles would be practically and appropriately applied within the context of how it actually will use data in the practical context of the organisation's business processes.

The guidance released April 17, 2012 by the privacy and information commissioners of Canada, British Columbia, and Alberta reflect the approach we suggest. The guidance entitled "Getting Accountability Right with a Privacy Management Program" which is attached as Annex A, provides discussion of this approach in more depth than is ventured in this letter.

Developing effective data protection law is a challenging endeavor. The Centre lauds your efforts and openness. We are hopeful that our comments will be helpful in your endeavor.

The Centre's comments will be short and will concentrate on two points:

1. The reliance on consent;
2. Assuring the Act protects Singapore citizens, residents and visitors without negatively impacting cloud computing or the processing of data that is already protected by laws in other regions.

Limitations of Consent as a Mechanism for Data Protection

Individuals should have control over the collection and use of the information that pertains to them when possible. However, data protection –protecting individuals from the risks to the person, financial and health matters, and reputation that comes from the misapplication of data - should not be built on the assumption that individuals will always have or exercise control over their data.

In a modern information economy data is not collected only directly from individuals, it is also collected from observation of individuals' behavior, individuals' interactions with others, and from calculations that come from data processing. Data is collected in person, on-line, through sensors built into streets, machines, and in remote locations. Today we generate as much data in two days as was generated in the first six thousand years of recorded history. Even the most attentive individual would have difficulty policing data practices based on his or her choices. Doing so would be a full time job.

Data protection law has historically been built based on the concept of individual control. That individual control was exercised via a notice that informs the individual of his or her choices and the mechanism for exercising consent. But even when it is centered an emphasis on consent, data protection law has always recognized the limitations of the approach. For example, European law does not rely on consent alone to establish a legal basis to process human resources data, because the power between the individual and organisation is not balanced, and true consent cannot always be achieved in the shadow of this imbalance.

The limitations of consent arise not only from the difference in the relative power between the individual and the organisation. There are also situations where consent is difficult or even impossible. For example, the observation of individuals by close circuit TV in a public location. Another example is where the smart phone is the primary interface between the individual and the organisation. There are also times when data is generated not from the individual's consenting, intentional actions, but rather from the individual's interaction with the environment or other individuals.

In this instance, the issue isn't the difficulty of gaining consent, as smart organisations will figure out how to get the necessary consents. The real problem for the individual is being comfortable there are effective protections for the individual from data driven risks.

Consent is very important, and should be sought where possible and effective. However the Singapore legislation should still allow for processing data where consent is impractical or ineffective. This, however, does not simply mean adding to a laundry list of situations where data may be processed without consent. Such a list will be out of date before the legislation even goes in to effect. Instead it means substituting effective responsibility for control of the data where consent is not workable. This is the modern concept of "accountability."[1]

The proposed European regulation creates a legal basis for processing based on legitimate business interest. However, it also obligates the organisation to balance its legitimate interests against the risks to the individual's fundamental rights and freedoms. This process of assessing risk is often referred to as "*privacy by design*," and is a component of accountability. The Canadian guidance mentioned earlier makes clear that a company has an obligation to conduct risks assessments and remain answerable for the integrity of the risk assessments they conduct.

The Centre would strongly recommend that Singapore recognize the changing nature of information flows and uses, reduce the burden on individuals, and give companies flexibility with regard to processing data while holding them responsible for protecting individuals from undo risks. The way to do so would emphasize consent where effective and possible, and in other cases require organisations to balance their legitimate business interests against the privacy risks to individuals.

Making Clear the Scope of the Legislation

The Centre was deeply involved in developing the APEC Data Privacy Framework. A clear guiding principle for that work was that obligations that come with personal data should stay with the data when it is processed in places ("non-home economies") outside the data's place of origin(the data's "home economy"), and that non-home economies where data is being processed should not add obligations beyond those needed to secure the data and respect the laws of the

[1] For further discussion about accountability, see "Data Protection Accountability: The Essential Elements: A Discussion Document, "Demonstrating and Measuring Accountability: A Discussion Document" and "Implementing Accountability in the Marketplace." See Appendix B-D and http://www.informationpolicycentre.com/accountability-based_privacy_governance.

home economy. The Centre believes the APEC position is correct, and believes it is also the intent of the Singapore data protection law.

Section 5 of the Act has the caption: "Act to apply only to personal data with a Singapore link." The Centre agrees with what we believe is the intent of this section, which is to cover data collected from Singapore residents or visitors. If that is indeed the intent, we are concerned that subsection (2)(a)(ii) of section 5 of the legislation doesn't achieve that end. The subsection says that the Singapore law would apply if the personal data was located in Singapore at the time of collection.

There are two problems with this language. First, if a company based outside Singapore outsources their website hosting to a company located in Singapore, then all data collected by the website would be subject to Singapore law when the law of the country where the company and possibly the individual reside is the appropriate governing law. Another example of this would be a call center located in Singapore receives a call from a Canadian or European citizen on behalf of a European company, Singapore law would apply when the Canadian or European law should be the governing one. Secondly, the terms "collected" and "located" are confusing. An example might be helpful. If a Canadian corporation has a fraud analytics center in Singapore, and shares data about its Canadian customers with that fraud center, would that sharing be a Singapore collection under this Act? Such a sharing would be subject to Canadian law. Could it also be subject to Singapore law?

The Centre does not believe that is your legislative intent, and suggests that you revisit the subsection in the draft legislation making it clear that data collected on individuals who reside outside Singapore and data collected under a service contract for a company located outside Singapore are only subject to appropriate security safeguards and to honoring the laws of the home-country. This would also be consistent with well-established principles of international law.

Conclusion

The Centre for Information Policy Leadership has participated in consultations on data protection world-wide for better than a decade. Policymakers are struggling with how to protect individuals while still encouraging innovation in an age when information is ubiquitous. This is doubly hard since data protection has often been equated with individual control. Individuals should have control over the information that pertains to them when possible. However, often that individual control via consent is not possible and/or practical. Accountability has begun to emerge as a way to assure protection when individual control is not possible. The Centre believes the Singapore legislation should reflect that trend, and be less reliant on consent.

The Singapore legislation is intended to cover the processing of data that pertains to residents and visitors to Singapore, and be respectful of the obligation that come with data from other jurisdictions. The Centre believes that assuring that result requires amendments to the exclusions contained in section 5.

If you have any questions related to these comments please feel free to contact Martin Abrams, President, Centre for Information Policy Leadership at mabrams@hunton.com.
Thank you for the opportunity to comment.

Office of the Information and Privacy Commissioner of Alberta

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Office of the Information & Privacy Commissioner for British Columbia

Getting Accountability Right with a Privacy Management Program

Purpose

The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia have worked together to develop this document with the goal of providing consistent guidance on what it means to be an accountable organization. It is intended for organizations subject to our respective private-sector privacy legislation and outlines what we expect to see in a privacy management program.

What is accountability?

Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organizations.

The concept of accountability appears straightforward, but constructing a privacy management program within an organization takes careful planning and consideration across disciplines and job functions. Employees of accountable organizations should be aware of and understand the applicable parts of the organization's privacy management program. Customers, partners, and service providers should likewise be made aware of and given confidence in relevant aspects of the privacy management program. Finally, accountable organizations should be able to demonstrate to Privacy Commissioners that they have an effective, up-to-date privacy management program in place in the event of a complaint investigation or audit. They will want to ensure that they are correctly identifying privacy-related obligations and risks and appropriately taking them into account in developing their business models and related technologies and business practices before they launch new products or services. They will want to

minimize risks to their organization and to their employees and customers, as well as mitigate the effects of any privacy breaches.

There will be times when mistakes are made. However, with a solid privacy management program, organizations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements.

This document outlines what we think are the best approaches for developing a sound privacy management program, for organizations of all sizes, in order to meet obligations under applicable privacy legislation. This document is not a "one-size-fits-all" solution, however. Each organization will need to determine, taking into consideration its size, how best to apply the guidance found here to develop a privacy management program. Public sector and health-care institutions will also find this document useful in establishing their own privacy management programs.

Part A of this document outlines "building blocks" or baseline fundamentals that every organization needs to have. Elements such as organizational commitment and program controls are essential.

Part B discusses how to maintain and improve a privacy management program on an ongoing basis. A privacy management program should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The building blocks must be monitored and assessed on a regular basis and be updated accordingly.

The end result is that the building blocks are always evolving to keep pace with changes both within and outside the organization. This could encompass changes in such areas as technology, business models, law and best practices.

In **Appendix A**, we include a list of the documents our respective offices have developed over the years that deal with different aspects of privacy compliance.

The Canadian Context

There are four statutory privacy regimes that may apply to the private sector in Canada. The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to federal works, undertakings or businesses (and to their employee personal information), and to provincially regulated businesses in provinces without substantially similar privacy legislation that collect, use or disclose personal information in the course

of commercial activities.[1] Three provinces have enacted private sector privacy laws which have been deemed by the Government of Canada to be "substantially similar" to PIPEDA – British Columbia, Alberta and Quebec.[2] British Columbia and Alberta have enacted *Personal Information Protection Acts* and Quebec has an *Act Respecting the Protection of Personal Information in the Private Sector*.[3]

The accountability principle is the first of 10 fair information principles under Schedule 1 of PIPEDA and is implicit in Alberta, British Columbia and Quebec's respective laws. It is the first among the principles because it is the means by which organizations are expected to give life to the rest of the fair information principles that are designed to appropriately handle and protect the personal information of individuals. (The full text of the accountability principle in Schedule 1 of PIPEDA is attached as **Appendix B**.)

International Context

The joint, federal-provincial nature of this guidance document is important given that personal information has become a global commodity, flowing constantly around the world, touched by organizations operating in multiple jurisdictions. The need for consistent approaches to personal information protection has never been greater.

Indeed, the global nature and the vast quantities of personal information flows have caused many privacy experts to examine in closer detail what it means for an organization to be accountable for protecting personal information. It has also caused experts to reflect further on how the concept of accountability can be leveraged to drive home the importance of protecting personal information in organizations in jurisdictions that may not have privacy legislation.

The accountability principle was first expressed in the Organisation for Economic Co-operation and Development's (OECD) 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, the first internationally agreed-to set of privacy principles. PIPEDA encompasses the Canadian Standards Association (CSA) Model Code (found in Schedule I of the Act), which was highly influenced by the OECD Guidelines. Since then, the accountability principle has been included in the Asia-Pacific Economic Cooperation's (APEC) Privacy Framework. Cross-border privacy

[1] PIPEDA, s. 26(2)(b)

[2] Organizations in the Province of British Columbia Exemption Order, SOR/2004-220; Organizations in the Province of Alberta Exemption Order, SOR/2004-219; Organizations in the Province of Quebec Exemption Order, SOR/2003-374.

[3] Three provincial statutes (in Ontario, New Brunswick and Newfoundland and Labrador) that regulate the handling of personal health information have substantially similar status.

rules are being developed within that region to implement the APEC Privacy Framework. These rules will elaborate on the principle of accountability.

The concept of accountability is also gaining interest within the European Union. The Article 29 Working Party Opinion on Accountability contains a thoughtful analysis of what accountability in privacy means and what might be expected of organizations in the future in demonstrating compliance, and puts forward a proposal that it believes should help "data protection move from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks." The European Commission has proposed a new European Union legal framework for privacy that contains a provision concerning accountability. Under it, organizations would be required to adopt policies and implement appropriate procedures to demonstrate that their processing of personal data is compliant with the proposed Regulation.

Apart from international agreements and domestic privacy law, Safe Harbor, self-certification programs, and Binding Corporate Rules are all examples of the use of the concept of accountability to promote privacy protection while supporting transborder data flows. The Accountability Project, an initiative led by the US-based Centre for Policy and Information Leadership, with participation from representatives of data protection authorities, business and academia, is examining what it means for an organization to be "accountable" for its privacy practices. The OPC and British Columbia Information and Privacy Commissioner have participated in this international initiative.

The benefits of implementing a privacy management program

Every organization that is subject to Canada's private-sector privacy laws is obliged to be in compliance with them. A comprehensive privacy management program provides an effective way for organizations to satisfy regulators and assure themselves that they are compliant. But it is more than that.

Such a program helps foster a culture of privacy throughout an organization. Senior management support is vital to achieving this goal. When senior management provides the needed resources to ensure appropriate training and education, risk assessment and monitoring, and auditing, it sends a clear signal that privacy is vital to the organization. In turn, a culture of privacy encourages employee support and reinforces the privacy protections the organization puts in place. When an organization takes the position that privacy is vital to its operations and "walks the talk" by implementing a robust privacy management program, enhanced trust that is essential for customers and clients to engage with that organization follows. An organization that has a strong privacy management program may enjoy an enhanced reputation that gives it a

competitive edge. In the longer term, a privacy management program that is scaled to the organization's needs will save money and make good business sense.

Conversely, without strong privacy protection, trust will erode to an organization's detriment. For example, privacy breaches are expensive for organizations – both in terms of "clean up" and reputation repair. Breaches may also prove expensive for the affected individuals. An appropriately designed and implemented privacy management program may help minimize the risk of such breaches, maximize the organization's ability to identify and address such incidents, and minimize their damage.

Given the vast amounts of personal information held by organizations and institutions, the increasing economic value of this information, and the heightened attention and concern regarding privacy breaches, it is vital that organizations take steps to develop and strengthen their privacy management programs to minimize risks and increase compliance.

Canadians expect and deserve it.

Part A Building Blocks

Accountability fundamentals: Developing a Comprehensive Privacy Management Program

What should an organization do to ensure that it is handling personal information appropriately? How will it know that it is doing it right? How will it be able to demonstrate to itself, its clients and to privacy commissioners that it has the capacity to comply and has complied with its legal obligations?

Accountability has a number of important requirements. Organizations are required to appoint someone to oversee the development, implementation and maintenance of the organization's privacy protection program. Policies and processes are needed, and training of employees required. Contracts (or other means) are required when organizations transfer personal information to third parties for processing, to ensure that the information in question is protected in a manner that is comparable to how the organization would protect it. Organizations are expected to have systems in place to respond to requests from individuals for access to (and correction of) their personal information, and they need to be able to respond to complaints from individuals about how personal information is being protected.

The OPC has developed a number of tools that will be of use to organizations to learn the basics about privacy and privacy legislation. These include: *Your Privacy*

Responsibilities: A Guide for Businesses and Organizations; *Privacy Questionnaire: Is Your Business Ready*? and a video for small- and medium-sized organizations entitled *PIPEDA for Business: What you need to know about protecting your customers' privacy*.

Alberta has developed the following documents which will be of assistance: *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights*; and *10 Steps to Implement PIPA*.

British Columbia has also developed similar tools relating to BC's private sector legislation including: *What are My Organization's Responsibilities Under PIPA?* and *A Guide for Business and Organizations to BC's Personal Information Protection Act*.

Part A will outline the building blocks that are essential components of a privacy management program that is demonstrably compliant with Canada's applicable private-sector privacy legislation.

1. Organizational commitment

This first building block is the development of an internal governance structure that fosters a privacy respectful culture.

Organizations are expected to develop and implement program controls that give effect to the privacy principles contained in the Federal, Alberta, and British Columbia private-sector privacy laws. Compliance with the laws, however, requires organizations to have a governance structure in place, with processes to follow and the means to ensure that they are being followed. Fundamentally, in order to be compliant and effective, a privacy-respectful culture needs to be cultivated.

a) Buy-in from the top

Senior management support is key to a successful privacy management program and essential for a privacy respectful culture.

When senior management is committed to ensuring that the organization is compliant with privacy legislation, the program will have a better chance of success, and a culture of privacy will more likely be established.

Senior management needs to actively champion the privacy program. It should:

- appoint the privacy point person(s) (Privacy Officer);
- endorse the program controls; and
- monitor and report to the Board, as appropriate, on the program.

Senior management will also need to provide support for the resources the program needs to succeed.

b) Privacy Officer

Organizations must appoint someone who is responsible for the privacy management program.

Whether this person is a C-level executive of a major corporation or the owner/operator of a very small organization, someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation. Other individuals may be involved in handling personal information, but the Privacy Officer is the one accountable for structuring, designing and managing the program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. Organizations should expect to dedicate some resources to training the Privacy Officer. The Privacy Officer should establish a program that demonstrates compliance by mapping the program to applicable legislation. It will be important to show how the program is being managed throughout the organization.

The Privacy Officer will play many roles with respect to privacy. S/he will:

- establish and implement program controls;
- coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
- be responsible for the ongoing assessment and revision of program controls;
- represent the organization in the event of a complaint investigation by a privacy commissioner's office; and
- advocate privacy within the organization itself.

This last role is as crucial as the others. Organizations face competing interests and privacy compliance is one program of many. Privacy, however, is more than a balancing of interests. Privacy should be seen in terms of improving processes, customer relationship management, and reputation. Consequently, the privacy management program's importance must be recognized at all levels.

It should be noted that an organization remains accountable for compliance with applicable privacy legislation. Appointing an individual to be responsible for the program does not negate the organization's accountability[4].

c) Privacy Office

For larger organizations, staff assigned to work on privacy issues will be needed.

[4] http://www.priv.gc.ca/cf-dc/2001/cf-dc_011204_e.asp

In larger organizations, the Privacy Officer will need to be supported by dedicated staff. The role of the Privacy Office must be defined and its resources must be identified and adequate. Staff of the Privacy Office should have delegated responsibilities to monitor compliance and foster a culture of privacy within the organization. The Office should also work to ensure that privacy protection is built into every major function involving the use of personal information, including product development, customer services or marketing initiatives.

d) Reporting

Reporting mechanisms need to be established, and reflected in the organization's program controls.

The organization needs to establish internal reporting mechanisms to ensure that the right people know how the privacy management program is structured and whether it is functioning as expected. Within fairly large organizations, the audience for this information is likely to be senior management, and in turn, senior management reports to the board of directors. All reporting mechanisms should be reflected in the organization's program controls.

Organizations should establish some form of internal audit and assurance programs to monitor compliance with their privacy policies. This could include the form of customer and employee feedback for smaller organizations, or for some larger organizations, third-party verifications. These reports will also help should the organization be subject to an investigation or audit under applicable privacy legislation as they are likely to demonstrate due diligence.

However, there is more to reporting than this. There will be times when privacy issues need to be escalated, for example, when there is a security breach or when a customer complains. Escalation means both involving people of relevant responsibility and ensuring that all the needed persons in the organization are included in the resolution of the issue. In large organizations, this could include, for example, representatives from technical, legal and corporate communications. How and when to escalate must be clearly defined and explained to all employees. To ensure that related processes are being followed, organizations will need to monitor whether the needed steps are being taken when triggered. Some organizations have found it useful to conduct test runs of their privacy breach identification, escalation and containment protocols, for example.

An effective reporting program:

- clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach;

- tests and reports on the results of its internal reporting structures; and
- documents all of its reporting structures.

2. Program controls

Program controls form the second building block. These help ensure that what is mandated in the governance structure is implemented in the organization. This section identifies the program controls in a privacy management program. Developing these controls will assist the Privacy Officer in structuring an appropriate privacy management program within the organization and the controls will be used to demonstrate how the program is compliant with privacy legislation.

a) Personal Information Inventory

Whether it has a sophisticated privacy management program in place or is implementing a new one, every organization can benefit from carefully examining the personal information it holds and how it currently handles this information.

An organization needs to know what personal information it holds, how it is being used – and whether it really needs it at all. Understanding and documenting the types of personal information that an organization collects and where it is held are critically important. This will affect the type of consent the organization obtains from individuals and how the information is protected; and it will make it easier to assist individuals in exercising their access and correction rights. Every component of an accountable, compliant privacy management program begins with this assessment.

Determining what is or is not personal information is not always a simple task, however. The OPC has issued an Interpretation on the definition of personal information, which organizations may find useful. It summarizes various court decisions and OPC findings on the definition. Whether sensitive (such as financial or health information) or not, all personal information must be appropriately safeguarded and only used for the purpose(s) for which it was collected. Sensitive information may require special treatment[5].

Every organization needs to determine:

- what personal information it holds and where it is held (within the organization or by third parties , for example) and document this assessment;

[5] Some personal information is almost always considered sensitive, such as financial or health information. Other personal information may be considered sensitive, depending on the context. Sensitive personal information may require greater safeguards and express consent.

- why it is collecting, using or disclosing personal information and document these reasons; and
- the sensitivity of the personal information it holds.

A document entitled *Securing Personal Information: A Self-Assessment Tool for Organizations*, issued by our Offices, also covers issues related to taking stock of personal information.

b) Policies

Organizations must develop and document internal policies that address obligations under the law. These policies need to be available to employees, and employees need to periodically sign off on them.

Organizations are required to develop internal policies that give effect to the principles contained in Canadian private-sector privacy legislation. These policies should be documented and should show how they connect to the applicable privacy legislation.

The key policies that organizations must have in place are the following:

i. Collection, use and disclosure of personal information, including requirements for consent and notification;
ii. Access to and correction of personal information;
iii. Retention and disposal of personal information;
iv. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls;
v. Challenging compliance.

Organizations should also incorporate privacy compliance requirements in other policies of the organization as appropriate. For example, in contract management policies, procurement policies, human resources policies and policies dealing with the disclosure of personal information to regulatory bodies, law enforcement agencies and internal security departments.

Organizations are required to develop internal policies that give effect to the principles contained in Canadian private-sector privacy legislation.

Each of the key policies is discussed below.

i. Collection, use and disclosure of personal information, which include requirements for consent and notification

It is important that employees understand their obligation to inform individuals of the reasons, and obtain their consent, for the collection, use and disclosure of personal

information. Privacy legislation requires that personal information only be collected, used or disclosed for appropriate purposes and limited to those purposes.

ii. Access to and correction of personal information

Employees need to understand that individuals have a right to access and correct personal information. Employees should understand how to help customers and employees exercise this right by knowing what processes to follow, including the timelines in which the organization must respond.

iii. Retention and disposal of personal information

In order to minimize unauthorized collection, use and disclosures, organizations should not retain personal information that is no longer required for the delivery of their services. Organizations must also have a policy regarding the disposal or destruction of records. Customers have the expectation that an organization will dispose of their personal information when it is no longer needed. As such, organizations should securely dispose of customers' records in accordance with its policy.

iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access

Organizations must protect the personal information they hold by making reasonable security arrangements. What is reasonable depends on the sensitivity of the information. For example, security arrangements could include locked filing cabinets, access controls and encryption to protect electronic databases. It is a very significant responsibility and, in most instances, requires specialized technical expertise to design an appropriate system.

Role-based access control is one of the best ways for organizations to limit who has access to what information. In accordance with "need to know" principles, employees should only have access to the minimum amount of personal information they need to perform their duties within the organization. Roles must be documented, remain up-to-date and assigned on a consistent basis, preferably by a central authority within the organization.

All three laws require that safeguards be in place to protect personal information.

The OPC, Alberta and British Columbia OIPCs have produced a document on securing personal information that is intended to help organizations, particularly small- and medium-sized enterprises, think about various aspects of their operations that may have

an impact on the security of personal information. We recommend that organizations review this tool.

v. Challenging compliance

Individuals have the right to challenge an organization's compliance with applicable privacy legislation. Organizations should therefore have internal policies in place for staff to follow in the event that individuals wish to complain about the organization's personal information handling practices.

c) Risk assessment tools

Privacy risks evolve over time. Conducting risk assessments, at least on an annual basis, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.

We have seen instances of organizations offering new services that collect, use or disclose personal information that have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a privacy problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any privacy impacts beforehand is vital.

As a result, such assessments should be required throughout the organization for all new[6] projects involving personal information and on any new collection, use or disclosure of personal information. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.

Organizations should develop procedures for conducting such assessments, and develop a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs. For larger organizations, the Privacy Officer should be aware of the review process, and where there are high-risk initiatives, services or programs, the Privacy Office should be directly involved.

d) Training and education requirements

A sound privacy management program requires all members of an organization to be aware of, and be ready to act on privacy obligations. Up-to-date training

[6] A new project may be modifying existing systems, components and processes.

and education requirements for all employees, tailored to specific needs, are key to compliance.

In order for a privacy management program to be effective, employees must be actively engaged in privacy protection. They need to be educated in privacy protection generally, and for those who handle personal information directly, they will need additional training specifically tailored to their roles. Training and education need to be recurrent, and the content of the program needs to be periodically revisited and updated to reflect changes.

Training and general education on privacy are very important. Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches.[7] In other cases, we have seen a lack of awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law.[8] In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.

Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection. Organizations may have very sound policies and program controls in place but if employees do not follow them, the privacy management program has broken down. Employees should be required to sign an agreement to comply with the organization's policies and program controls.

There are numerous ways for organizations to deliver training and general privacy education. Examples include, providing mandatory training modules on the company intranet, small group sessions, one-on-one training, monthly e-newsletters, or inserting modules within training on organization policies. The organization should document its training processes and measure participation and success.

For privacy training and education to be effective, it must:

- be mandatory for all new employees before they access personal information and periodically thereafter;
- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs; and

[7] For an example, see http://www.priv.gc.ca/cf-dc/incidents/2005/050418_01_e.asp.
[8] For an example, see http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.asp, involving Google's collection of personal information from unencrypted wifi networks.

- circulate essential information to relevant employees as soon as practical if an urgent need arises.

e) Breach and incident management response protocols

Risk assessments, both internal and external, may help mitigate privacy breaches, which are unfortunately becoming a frequent fixture in the news. As previously noted, breaches are expensive on many fronts and taxing on consumer trust.

As a result, organizations should have a procedure in place and a person responsible for managing a personal information breach. For larger organizations, a collaborative approach may be required, with employees from different parts of the organization working together. Responsibilities for internal and external reporting of the breach must be clear.

In Alberta, an organization that has personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

Reporting to privacy commissioners and notification of affected individuals may also be required. Organizations operating in Alberta or collecting personal information of Alberta residents are required by law to report certain breaches to the Information and Privacy Commissioner of Alberta. Regardless of whether reporting is mandatory or not in a particular jurisdiction, organizations are encouraged to report breaches to the appropriate offices.

For more guidance on the expectations regarding breaches, please see BC's *Privacy Breach Checklist*; *Breach Notification Assessment Tool*; and *Key Steps in Responding to Privacy Breaches*; Alberta's *Reporting a Breach to the Commissioner*; *Breach Report Form*; *Notifying Affected Individuals*; and the OPC's *Privacy Breach Handbook*.

f) Service provider management

Personal information handling by third parties is another key area to consider. Are there contractual or other means in place to protect that personal information? Is the information leaving the country? If so, has the organization taken into consideration the sensitivity of the information and the requirements of the foreign regime? The OPC's *Guidelines for Processing Personal Data Across Borders* provides additional information on accountability and the use of third-party processors and trans-border data flows.

Such considerations are part of assessing risk. At a minimum, privacy requirements for service providers should include the following:

- privacy provisions in contracts setting out requirements for compliance including binding the service provider to the policies and protocols of the organization and requiring the organization to be notified in the event of a breach;
- training and education for all service provider employees with access to personal information;
- sub-contracting;
- audits; and agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.

The law stipulates that the organization that is transferring personal information to a third party for processing remains responsible for the personal information. Contractual or other means may be used to provide protection; policies and procedures may need to include information on where the information is going and why.

g) External communication

Organizations also have to develop a procedure for informing individuals of their privacy rights and the organization's program controls. This external communication should be clear and understandable and not simply a reiteration of the law. It should:

- provide enough information so that the public knows the purpose of the collection, use and disclosure of personal information as well as how it is safeguarded and how long it is retained;
- notify individuals if their personal information is being transferred outside of Canada;
- include information on who to contact with questions or concerns; and
- be made easily available to individuals.

Individuals should be made aware of their ability to access their personal information held by the organization, and how to request correction or to complain about the organization's privacy compliance, including the right to challenge the organization's actions by submitting a complaint to the Privacy Commissioner.

The OPC has developed a number of documents that are useful for organizations developing internal policies and external communication. These include: *Build a Privacy Plan for your Business*; *PIPEDA Self-Assessment Tool*; *Privacy Guide for Small Businesses: The Basics*; *Guidelines for Processing Personal Data Across Borders*; *Privacy and Your Business: Privacy Breach Handbook*; and *Your Privacy Responsibilities: A Guide for Businesses and Organizations*.

Alberta has developed the following documents: *Key Steps in Responding to Privacy Breaches*; *PIPA Advisory 2: Access Requests: An Overview*; *PIPA Advisory 3: Access Requests: Responding to a Request*; and *PIPA Advisory 8: Access Requests: Reasonable Safeguards*.

British Columbia's resources include: *Privacy Breach management Policy Template; Key Steps in Responding to Privacy Breaches*; *Breach Notification Assessment tool* and *PIPA and the Hiring Process*.

Part B Ongoing Assessment and Revision

Part A describes the building blocks of creating a privacy management program. Part B of this document outlines the critical tasks involved in the maintenance of a privacy management program to ensure ongoing effectiveness, compliance and accountability. In order to properly protect privacy and meet legal obligations, organizations must monitor, assess and revise their framework to ensure it remains relevant and effective. In order to accomplish this work, sufficient resources and training must be allocated to the Privacy Officer.

1. Develop an Oversight and Review Plan

An oversight and review plan will help the organization keep its privacy management program on track and up to date.

The Privacy Officer should develop an oversight and review plan on an annual basis that sets out how and when s/he will monitor and assess the organization's privacy management program's effectiveness, as outlined in organizational commitments. The plan should establish performance measures and include a schedule of when all policies and other program controls will be reviewed.

2. Assess and Revise Program Controls

The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.

Monitoring is an ongoing process and should address at a minimum the following questions:

- what are the latest threats and risks?

- are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the privacy commissioners?
- are new services being offered that involve increased collection, use or disclosure of personal information?
- is training occurring, is it effective, are policies and procedures being followed, and is the program up to date?

If there are problems found during the monitoring process, concerns will need to be documented and addressed by the appropriate officials.

For critical or high-risk processes, periodic internal or external audits are important ways to assess the effectiveness of an organization's privacy program. However, at a bare minimum, the Privacy Officer should conduct periodic assessments to ensure key processes are being respected. For smaller organizations or for less formal reviews, organizations should develop checklists that are reviewed on a regular basis. Through whatever means appropriate,, organizations need to ensure that employees or contractors are following the organization's policies and program controls.

As noted earlier, this document is not a "one-size-fits-all" solution. Each organization will need to decide how to structure its own privacy management program, taking into consideration a number of factors, including the size of the organization, and the amount and sensitivity of the personal information it handles.

When organizations begin developing their privacy management programs, they may not have in place every element of a compliant program. Even organizations with fairly mature programs need to ensure that they are taking reasonable steps to maintain compliance. It is important for any organization to gauge progress through the use of metrics, with continued compliance being the objective.

The expectation is that an organization conducts assessments of its program controls (as outlined in Part A) in a focused, continuous and thorough manner.

Based on the results of the assessment process, the Privacy Officer must consider whether to take action to update and revise the program controls. This is a critical responsibility. The changes must be communicated to employees either as they are made or in "refresher" education and training modules.

In short, the following actions will need to be undertaken by the Privacy Officer:

a) **monitor and update personal information inventory** continuously to keep it current and identify and evaluate new collections, uses and disclosures;

b) **review and revise policies** as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices, or as a result of environmental scans. The importance of this work cannot be overstated. There is no point in having policies if they are not effective and relevant – or if nobody within the organization knows about them.

c) **treat privacy impact assessments and security threat and risk assessments as evergreen documents** so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.

d) **review and modify training and education** on a periodic basis as a result of ongoing assessments and communicate changes made to program controls.

e) **review and adapt breach and incident management response protocols** to implement best practices or recommendations and lessons learned from post-incident reviews.

f) **review and**, where necessary, **fine-tune** requirements in contracts with **service providers.**

g) **update and clarify external communication** explaining privacy policies.

Conclusion

Demonstrating Compliance

Accountable organizations are able to demonstrate that they have a comprehensive privacy management program in place.

This document outlines the elements and strategies of a privacy management program that can help organizations "get accountability right". With such a program, organizations will be able to demonstrate to customers, employees, partners, shareholders, and privacy commissioners that they have in place a robust privacy compliance program. They will be able to describe and document all of the elements outlined in this guidance document and show evidence of how they have implemented their program.

Should there be an investigation by a Privacy Commissioner's office regarding a complaint about a possible contravention of the law or an audit of your practices, an organization may be asked to show how it addresses the requirements of the applicable law. The Privacy Officer needs to have the program fully documented in the event of such an occurrence. During an investigation or audit, our Offices will expect that

organizations can demonstrate that they have an up-to-date, comprehensive privacy program in place. Evidence of an effective privacy management program assists Commissioners in determining whether or not the organization has reasonable safeguards in place, and has complied with the accountability requirements under applicable law.

Organizations that do not meet that expectation will find themselves faced with additional work to establish or update such a program.

Beyond the law – Why privacy should matter to business

Within an organization, privacy is essential to establishing and maintaining trust. If customers, clients or employees believe that their personal information will be handled respectfully, in an open and transparent manner, with strong, reasonable safeguards, and made accessible to them at their request, this fosters trust and a continued positive relationship can be expected. If customers are typically considered a business' greatest asset, then their personal information must be considered one as well. Organizations will want to build and protect their assets, and personal information, as an asset, is no different.

An accountable organization can demonstrate to customers, employees, shareholders, regulators, and competitors that it values privacy, not only for compliance reasons, but also because privacy makes good business sense. It is hoped that the guidance contained in this document will help all organizations achieve that goal.

Privacy Management Program - At A Glance

A. Building Blocks

Organizational Commitment	**a) Buy-in from the top**	Senior management support is key to a successful privacy management program and essential for a privacy respectful culture.
	b) Privacy Officer	• Role exists and is fundamental to business decision-making process. • Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the organization. • Responsible for the development and implementation of the program controls and their ongoing assessment and revision.
	c) Privacy Office	• Role is defined and resources are identified and adequate. • Organizational structure supports the ability of staff to monitor compliance and foster a culture of privacy within the organization. • Ensures privacy protection is built into every major function involving the use of personal information.
	d) Reporting	Reporting mechanisms need to be established, and they need to be reflected in the organization's program controls.
Program Controls	**a) Personal Information Inventory**	The organization is able to identify: • the personal information in its custody or control, • its authority for the collection, use and disclosure of the personal information, and the sensitivity of the personal information.

	b) Policies	i. Collection, use and disclosure of personal information, which include requirements for consent and notification ii. Access to and correction of personal information iii. Retention and disposal of personal information iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access v. Challenging compliance
	c) Risk Assessment Tools **d) Training and education requirements** **e) Breach and incident management response protocols** **f) Service Provider management** **g) External communication**	

B. Ongoing Assessment and Revision

Oversight and Review Plan	**a) Develop an oversight and review plan**	Privacy Officer should develop an oversight and review plan on an annual basis that that sets out how s/he will monitor and assess the effectiveness of the organization's program controls.
Assess and Revise Program Controls As Necessary	**a) Update personal information inventory** **b) Revise policies** **c) Treat risk assessment tools as evergreen** **d) Modify training and education** **e) Adapt breach and incident response protocols** **f) Fine-tune service provider management** **g) Improve external communication**	

Appendix “A”

Materials prepared by the Offices of the Privacy Commissioner of Canada, the Alberta Information and Privacy Commissioner, and the British Columbia Information and Privacy Commissioner, cited in the guidance document

List of Materials Prepared by the Office of the Privacy Commissioner of Canada

General Information for Business on Privacy:

Your Privacy Responsibilities: A Guide for Businesses and Organizations
http://www.priv.gc.ca/information/guide_e.asp

Privacy Questionnaire: Is Your Business Ready?
http://www.priv.gc.ca/resource/tool-outil/ekit/quest_01_e.asp

PIPEDA for Business: What you need to know about protecting your customers' privacy
(video for small- and medium-sized businesses)
http://www.priv.gc.ca/resource/videos/2010/bus_2010_index_e.asp

Interpretations:

Accountability
http://www.priv.gc.ca/leg_c/interpretations_02_acc_e.asp

Personal Information
http://www.priv.gc.ca/leg_c/interpretations_02_e.asp

Privacy Breaches:

Privacy Breach Handbook
http://www.priv.gc.ca/resource/pb-avp/pb_hb_e.asp

Transborder Flows of Personal Information/Outsourcing:

Guidelines for Processing Personal Data Across Borders
http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

Internal Policies and External Communications:

Build a Privacy Plan for your Business
http://www.priv.gc.ca/resource/tool-outil/english/index.asp?a=logout

PIPEDA Self-Assessment Tool
http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp

Privacy Guide for Small Businesses: The Basics
http://www.priv.gc.ca/information/pub/guide_sb_e.asp

Guidelines for Processing Personal Data Across Borders
http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

Privacy and Your Business: Privacy Breach Handbook
http://www.priv.gc.ca/resource/pb-avp/pb_hb_e.asp

Your Privacy Responsibilities: A Guide for Businesses and Organizations
http://www.priv.gc.ca/information/guide_e.asp

List of Materials Prepared by the Alberta Office of the Information and Privacy Commissioner

General Information for Business on Privacy:

Guide for Businesses and Organizations on the Personal Information Protection Act
http://www.oipc.ab.ca/Content_Files/Files/Publications/PIPAguide_Nov2008_web.pdf

Information Privacy Rights
http://www.oipc.ab.ca/Content_Files/Files/Publications/Information_Privacy_Right_2007.pdf

10 Steps to Implement PIPA
http://servicealberta.ca/pipa/documents/ImplementPIPA.pdf

Privacy Breaches:

Reporting a Breach to the Commissioner
http://www.oipc.ab.ca/Content_Files/Files/Publications/Reporting_a_Breach_to_the_Commissioner.pdf

Breach Report Form
http://www.oipc.ab.ca/Content_Files/Files/Publications/Breach_Report_Form_2010.pdf

Notifying Affected Individuals

http://www.oipc.ab.ca/Content_Files/Files/Publications/Notifying_Affected_Individuals.pdf

Internal Policies and External Communications:

Key Steps in Responding to Privacy Breaches
http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf

PIPA Advisory 2: Access Requests: An Overview
http://www.oipc.ab.ca/Content_Files/Files/Publications/2JCRightofAccessRequestsAnOverviewApr2007.pdf

PIPA Advisory 3: Access Requests: Responding to a Request
http://www.oipc.ab.ca/Content_Files/Files/Publications/3_JC_Right_of_Access_Requests_Responding_to_a_Request_Apr2007.pdf

PIPA Advisory 8: Access Requests: Reasonable Safeguards
http://www.oipc.ab.ca/Content_Files/Files/Publications/PIPA_Advisory_8_Reasonable_Safeguards2007.pdf

List of Materials Prepared by the British Columbia Office of the Information and Privacy Commissioner

General Information for Business on Privacy:

What are My Organization's Responsibilities Under PIPA?
http://www.oipc.bc.ca/index.php?option=com_content&view=article&catid=17%3Aprivate-sector-pages&id=73%3Aprivate-sector-g-what-are-my-organizations-responsibilities-under-pipa&Itemid=78

A Guide for Business and Organizations to BC's Personal Information Protection Act.
http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA%283rd_ed%29.pdf

Privacy Breaches:

Privacy Breach Checklist
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist%28June2008%29.pdf

Breach Notification Assessment Tool
http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf

Key Steps in Responding to Privacy Breaches

http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches%28June2008%29.pdf

Internal Policies and External Communications:

Privacy Breach management Policy Template
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Management_Policy_Template%28June2008%29.pdf

Key Steps in Responding to Privacy Breaches
http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches%28June2008%29.pdf

Breach Notification Assessment tool
http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf

PIPA and the Hiring Process
http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ(10APR06).pdf

Jointly issued guidance:

Securing Personal Information: A Self-Assessment Tool for Organizations
http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Appendix “B”

The accountability principle in Schedule 1 of PIPEDA reads as follows:

4.1 Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organizations’ compliance with the following principles.

4.1.1

Accountability for the organizations’ compliance with the principles rests with the designated individuals(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individuals(s).

4.1.2

The identity of the individuals(s) designated by the organization to oversee the organizations’ compliance with the principles shall be made known upon request.

4.1.3

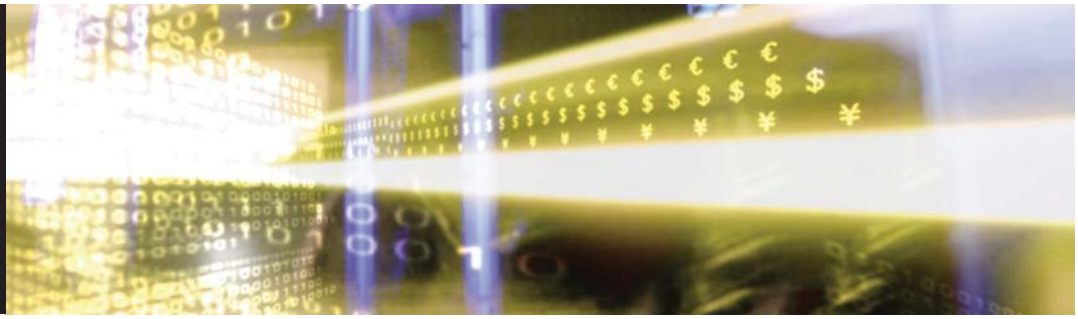
An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(a) Implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training employees on and communicating information about the organization’s policies and practices; and
(d) developing information to explain the organization’s policies and procedures.

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



Data Protection Accountability: The Essential Elements
A Document for Discussion
October 2009

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Galway Project

Data Protection Accountability: The Essential Elements
A Document for Discussion

Preface

Martin Abrams
Executive Director
Centre for Information Policy Leadership

Innovations in technology; rapid increases in data collection, analysis and use; and the global flow and access to data have made an unprecedented array of products, resources and services available to consumers. These developments, however, in no way diminish an individual's right to the secure, protected and appropriate collection and use of their information.

The manner in which those protections are provided is often challenged by the dynamic, increasingly international environment for information. The global flow of data tests existing notions of jurisdiction and cross-border co-operation. How can companies and regulators support movement of data while providing the protections guaranteed to the individual?

Accountability, a concept first established in data protection by the Organisation for Economic Co-operation and Development ("OECD"), may provide an improved approach to transborder data governance that encourages robust data flows and provides for the protection and responsible use of information, wherever it is processed. But the practical aspects of accountability, and how it can be used to address the protection of cross-border information transfers, have not been clearly articulated.

- What will be expected of companies in an accountability system?
- How will enforcement agencies monitor and measure accountability?
- How can the protection of individuals be ensured?

The Centre for Information Policy Leadership at Hunton & Williams LLP was privileged to assemble a group of international experts from government, industry and academia to consider how an accountability-based system might be designed.[1] The experts met twice to define the essential elements of accountability, examine issues raised by the adoption of the approach and propose additional work required to facilitate establishment of accountability as a practical and credible mechanism for information governance. This report, guided by a drafting committee and reviewed by the group of experts, reflects the results of those deliberations.

[1] The group of experts is listed in the Appendix.

While this paper is focused on accountability as a mechanism for global governance of data, the issue of how accountability relates to the general oversight of privacy was raised during our discussions. It may be that accountability principles can address both international as well as domestic protection of information. Our discussion recognised that the concepts of accountability that can support an improved approach already are reflected in long-standing principles of fair information practices and are inherent in current governance in Europe, Asia and North America. Making accountability a reality requires that businesses apply those concepts so that their management of information is both safe and productive. Our talks further suggested that the growing complexity of data collection and use requires that much of the burden for protecting data must shift from the individual to the organisation.

Much of what is written about accountability in this paper can be accomplished by reinterpreting existing law. It is our hope that this paper will both chart the course forward for establishing accountability-based protection and motivate stakeholders to take the important steps to do so.

The Centre is indebted to the experts who participated in this effort for generously giving of their time and expertise, and most especially to the Office of the Data Protection Commissioner of Ireland for hosting our meetings and providing us with wise guidance. While this report reflects the results of their deliberations, the Centre alone is responsible for any errors in this paper.

Executive Summary

Accountability is a well-established principle of data protection. The principle of accountability is found in known guidance such as the OECD Guidelines[2]; in the laws of the European Union ("EU"), the EU member states, Canada and the United States; and in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. Despite its repeated recognition as a critical component of effective data protection, how accountability is demonstrated or measured has not been clearly articulated. This paper represents the results of the Galway Project — an effort initiated in January 2009 by an international group of experts from government, industry and academia to define the essential elements of accountability and consider how an accountability approach to information privacy protection would work in practice.

Accountability does not redefine privacy, nor does it replace existing law or regulation; accountable organisations must comply with existing applicable law. But accountability shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to

[2] Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

determine appropriate, effective measures to reach those goals. As the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability to make decisions to control the use and sharing of information through active choice, accountability requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to ensure responsible decision-making about the management and protection of data. The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

3. **Systems for internal, ongoing oversight and assurance reviews and external verification.**

4. **Transparency and mechanisms for individual participation.**

5. **Means for remediation and external enforcement.**

While many aspects of the essential elements are already established in law, self-regulation and corporate practices, some issues remain to be resolved to encourage robust adoption of an accountability approach. Policymakers and stakeholders should address questions about how accountability would work with existing legal regimes, and whether reinterpretation or amendment of existing laws might be required to make it possible to hold organisations accountable. Third-party accountability programmes have been recognised as useful in supplementing the work of government agencies. As they may play an important part in the administration of this approach, it will be necessary to clearly describe the contours of their role and the criteria by which their credibility will be assessed. Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. For the approach to work effectively, stakeholders must articulate the way in which the credibility of those programmes is established and tested. Finally, small- and medium-sized enterprises that wish to demonstrate accountability will face specific challenges that must be addressed.

While additional inquiry is needed before adoption of an accountability-based approach can be realised, its promise for international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates — robust transfer and use of data in a fashion that is responsible and protected.

Introduction

The global flow of data drives today's information economy. Innovation, efficiency and service depend on rapid and reliable access to data, irrespective of its location. Digital technologies collect and store data in ways never before imagined, and information and telecommunications networks have evolved to provide seamless, low-cost access to data around the world.

As a result consumers have access to an unprecedented array of personalised products and services. While previously service hours ended at 5:00 p.m., the Internet enables individuals to access customer service in the middle of the night by phoning a local number that connects them to a call centre a continent away. Today, on a single server, a company can manage its email and business records for offices located in a dozen nations; travelers can rely on their debit and credit cards wherever they go; and individuals can use the Internet to download information from around the world without ever leaving their homes.

Indeed, with the increasingly global nature of data flows and the remote storage and processing of data in the "cloud", geography and national boundaries will impose few limitations on where data can be transferred but will present more practical challenges for administering and supervising global businesses.

In this environment, individuals maintain the right to the secure and protected processing and storage of their data that does not compromise their privacy. Protection must be sufficiently flexible to allow for rapidly changing technologies, business processes and consumer demand. Regulators must be equipped to articulate clear requirements for protection, educate companies and citizens, and monitor compliance in an environment in which data processing increasingly occurs outside the practical reach of most regulators, if not their legal jurisdiction.

Currently, global data flows are governed by law and guidance, which are enacted and enforced by individual countries or through regionally adopted directives or agreed-upon principles. The EU Data Protection Directive and implementing laws of member states, for example, govern the transfer of data from the European Union. The Safeguards Rule[3] imposes legal obligations on U.S. organisations to ensure that data is properly secured, wherever it is transferred or processed. And yet global data flows often challenge the way in which we have traditionally approached information protection. Daniel Weitzner and colleagues have written that information protection policy has long relied on attempts to keep information from " 'escaping' from beyond appropriate boundaries".[4] This approach is plainly inadequate in a highly connected environment in which anyone armed with a cell phone or laptop has at his or her fingertips unprecedented processing power, as well

[3] Under the Gramm-Leach-Bliley Act, the Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information.

[4] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Jay Sussman, "Information Accountability," *Communications of the ACM*, June 2008, at 82.

as the practical ability to collect, aggregate, transfer and use personal data around the world — and in an environment in which those capabilities are growing exponentially.

Weitzner and his colleagues lead a growing multinational call for an alternative approach to securing and governing personal data based on *accountability*. An accountability-based approach to data protection requires that organisations that collect, process or otherwise use personal data take responsibility for its protection and appropriate use beyond mere legal requirements, and are accountable for any misuse of the information that is in their care.

Adoption of an accountability-based approach to governance of privacy and information in global data flows raises significant questions for business, government and individuals.

Businesses express concerns about what might be expected of them in an accountability system, how their efforts to meet those expectations will be measured and how the rules related to accountability will be defined and enforced. Privacy enforcement agencies ask how accountability might work under local law. How do enforcement agencies measure an organisation's willingness and capacity to protect information when it is no longer in the privacy protection agency's jurisdiction? How does the agency work with and trust agencies in other jurisdictions? Consumer advocates worry that accountability will lessen the individual's ability to make his own determination about appropriate use of information pertaining to him.

The Centre for Information Policy Leadership, through a process facilitated by the Office of the Irish Data Protection Commissioner, convened experts to define the essential elements of accountability; to explore the questions raised by government, business and consumers related to adoption of an accountability approach; and to suggest additional work necessary to establish accountability as a trusted mechanism for information governance.

A small group of experts met initially in January 2009 to define the contours of the inquiry and identify existing research and legal precedents involving accountability. That meeting led to a draft paper that was presented to a larger gathering in April that included data protection experts drawn from government, industry and academia from ten countries. The April meeting identified a drafting committee that oversaw the Centre staff as they prepared this document, which was then circulated for comment among all of the participants. This paper reflects the results of that process.

Accountability in Current Guidance

Accountability as a principle of data protection is not new. It was established in 1980 in the OECD Guidelines[5] and plays an increasingly important and visible role in privacy

[5] See, Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

governance. The Accountability Principle places responsibility on organisations as data controllers "for complying with measures that give effect" to all of the OECD principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly stated in the Directive, numerous provisions require that organisations implement processes that assess how much data to collect, whether the data may be appropriate for a specified purpose and the level of protection necessary to ensure that it is secure. Accountability also has featured more prominently in data governance in Europe as binding corporate rules have served as a mechanism to ensure the trusted transfer of personal data outside the EU.

The Spanish Data Protection Agency's February 2009 Joint Proposal for an International Privacy Standard includes an accountability principle that establishes a basis for data transfers based on an organisation's demonstration that it is responsible.[6]

Accountability is also the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), requiring that Canadian organisations put into effect the full complement of PIPEDA principles, whether the data are processed by the organisation or outside vendors, or within or outside Canada. In doing so, the accountability principle of PIPEDA establishes in law a governance mechanism for transborder data transfers.[7]

In the United States, the Federal Trade Commission ("FTC") applies to general commerce the Safeguards Rule of the Gramm-Leach-Bliley Act ("GLBA") — an accountability-based law that places obligations on a financial services organisation to ensure personal information is secured, but that does not explicitly explain how those obligations should be met.

The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework includes accountability as an explicit principle,[8] basing it on the OECD language and applying it to data transfers beyond national borders. The Framework states, "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above." The Framework specifically requires such accountability "when personal information is to be transferred to another person or organisation, whether domestically or internationally."

---

[6] "Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Information," version 2.3, 24 February 2009.

[7] This governance was explicitly described in a 2009 publication of the Office of the Privacy Commissioner of Canada, "Processing Personal Data Across Borders: Guidelines". In PIPEDA, accountability is an overarching principle that applies to protection and management of data, whether it is maintained and processed domestically or transferred outside Canadian borders for storage and processing.

[8] For more information about the APEC Privacy Framework and a full articulation of the principles, see <.<http://www.apec.org_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html#>.

Despite the inclusion of accountability in many data protection regimes, it is often unclear how companies demonstrate accountability for purposes of cross-border data transfers, how regulators measure it or why individuals should trust it.

What is an Accountability-based Approach?

An accountability-based approach to data governance is characterised by its focus on setting privacy-protection goals for organisations based on criteria established in current public policy and on allowing organisations discretion in determining appropriate measures to reach those goals. An accountability approach enables organisations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customers.

An accountability-based approach to privacy protection offers immediate advantages to individuals, institutions and regulators alike, because it recognises and is adaptable to the rapid increases in data flows.

- It will help bridge approaches across disparate regulatory systems, by allowing countries to pursue common data protection objectives through very different — but equally reliable — means. This helps to facilitate the many benefits of allowing data to move across borders, and to assure individuals a common level of data protection — even if achieved through a variety of means — irrespective of where their information is located.

- It will also heighten the confidence of individuals that their data will be protected wherever it is located and minimise their concerns about jurisdiction or local legal protections.

- It will raise the quality of data protection, by allowing use of tools that best respond to specific risks and facilitating the rapid updating of those tools to respond quickly to new business models and emerging technologies. An accountability approach requires organisations not only to take responsibility for the data they handle but also to have the ability to demonstrate that they have the systems, policies, training and other practices in place to do so.

- Allowing for greater flexibility will enable organisations to more effectively conserve scarce resources allocated to privacy protection. While it is essential that an accountable organisation complies with rules, resources devoted to fulfilling requirements such as notification of data protection authorities are not available for other, often more effective, protection measures. Accountability directs scarce resources towards mechanisms that most effectively provide protection for data. Organisations will adopt the tools best suited to guarantee that protections focus on reaching substantive privacy outcomes — measurable information protection goals — and to demonstrate their ability to achieve them.

Accountability does not redefine privacy, nor does it replace existing law or regulation. Accountable organisations must comply with existing applicable law, and legal mechanisms to achieve privacy goals will continue to be the concern of both regulators and organisations. However, an accountability approach shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified objectives.

Accountability does not replace principles of individual participation and consent that have been well established in fair information practices.[9] In many cases, consumer consent to uses of data remains essential to an organisation's decisions about data management. However, in some instances obtaining such consent may be impossible or highly impractical, and an accountability approach requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

How Accountability Differs from Current Approaches

Accountability is designed to provide robust protections for data while avoiding aspects of current data protection regimes that may be of limited effect or that may burden organisations without yielding commensurate benefits. Accountability allows the organisation greater flexibility to adapt its data practices to serve emerging business models and to meet consumer demand. In exchange, it requires that the organisation commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a fashion that protects information and the individuals to which it pertains. Accountability requires an organisation to remain accountable no matter where the information is processed. Accountability relies less on

---

[9] Consent is found in the OECD Guidelines principle of Use Limitation, which states: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."

The principle of individual participation is also found in the OECD Guidelines, which state:

"An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

the rules that exist where the data is processed and more where the obligation is first established.[10]

Accountability relies less on specific rules but instead requires that organisations adopt policies that align with external criteria found in law — generally accepted principles or industry best practices — and foster a level of data protection commensurate with the risks to individuals raised by loss or inappropriate use of data. The accountable organisation complies with applicable law and then takes the further step to implement a programme that ensures the privacy and protection of data based on an assessment of the risks to individuals raised by its use. These risks should be assessed and measured based on guidance from regulators, advocates, individuals and other members of industry. Ultimately, regulators are responsible for ensuring that the risks to the data have been managed appropriately.

While the individual continues to play an important role in protecting his or her information, accountability shifts the primary responsibility for data protection from the individual to the organisation collecting and using data. Much of United States law, for example, is based on disclosure of the organisation's privacy policy, notification of individuals and obtaining their consent to specific uses of data. This approach is designed to enhance individual control over the manner in which data is used. Individuals are vested with responsibility for determining the manner in which their data is used and shared; organisations are obligated to provide the individual with sufficient information on which to base an informed choice.

In the U.S. the Federal Trade Commission is authorised to bring an enforcement action based on the organisation's notice when an organisation acts in an unfair or deceptive manner with respect to its privacy practices. In the absence of, and in some cases even with, an overarching privacy law, the individual is charged with policing the marketplace for privacy, by familiarising him- or herself with every organisation's policy and making a decision based on that information whether or not the organisation is trustworthy and using data in an appropriate manner.

Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing the marketplace for enterprises using data irresponsibly. Faced with rapid advances in data analytics and increasingly complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions, even when they can access privacy policies. Accountability demands responsible, appropriate data use whether or not a consumer has consented to one particular use or another.

Accountability does not wait for a system failure; rather, it requires that organisations be prepared to demonstrate upon request by the proper authorities that it is securing and protecting data in accordance with the essential elements.

[10] When, however, information security rules where data are processed are stronger than where the security obligation was incurred, they may indeed apply.

Enforcement of binding corporate rules ("BCRs") or the cross-border privacy rules as defined in APEC perhaps most closely approximate an accountability approach to information management and protection. BCRs, which are more fully developed, provide a legal basis for international data flows within a corporation or a group of organisations when other options are either impracticable or of limited utility. BCRs are a set of rules, backed by an implementation strategy, adopted within a company or corporate group that provides legally binding protections for data processing within the company or group. While the Directive and national laws that implement it rely on adequacy of laws and enforcement in a particular legal jurisdiction outside the EU, BCRs allow companies to write rules for data transfer that are linked to the laws where data was collected rather than look to compliance with the law of a particular geographic location where the data may be processed. Data authorities examine whether an organisation's binding rules export local European law with the data, and can determine whether its data practices and protections can be trusted to put those rules into effect — that it has in place the procedures, policies and mechanisms necessary to meet the obligations established in the BCR and to monitor and ensure compliance.[11]

Essential Elements of Accountability

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

   An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices. An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by

[11] BCRs cover only governance of data originating in the European Union. They do not apply to data originating from other regions.

tasking appropriate staff with implementing the policies and overseeing those activities.

Many global organisations have established policies in accordance with accepted external criteria such as the EU Directive, OECD Guidelines or APEC Principles. These companies demonstrate high-level commitment to those policies and the internal practices that implement them by requiring their review and endorsement by members of the organisation's executive committee or board of directors.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

Organisations in Europe, North America and Asia-Pacific have implemented comprehensive privacy programmes that incorporate personnel training, privacy impact assessments and oversight. In some cases, organisations have automated processes and integrated responsibility for programme obligations into all levels and across all aspects of the enterprise, while responsibility for compliance, policy development and oversight remains in the privacy office.

3. Systems for internal ongoing oversight and assurance reviews and external verification.

Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful — and must be subject to some form of monitoring.[12]

[12] Accountable organisations have traditionally established performance systems based on their own business culture. Successful performance systems share several characteristics:

- they are consistent with the organisation's culture and are integrated into business processes;

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.

The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution. External verification must be both trustworthy and affordable. Privacy officers may work with their audit departments to ensure that internal audits are among the tools available to oversee the organisation's data management. Organisations may also engage firms to conduct formal external audits. Seal programmes[13] in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.

4. Transparency and mechanisms for individual participation.

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also

---

- they assess risk across the entire data life cycle;
- they include training, decision tools and monitoring;
- they apply to outside vendors and other third parties to assure that the obligations that come with personal data are met no matter where data is processed;
- they allocate resources where the risk to individuals is greatest; and
- they are a function of an organisation's policies and commitment.

[13] Seal programmes are online third party accountability agents.

provides for those instances when it is feasible. In such cases it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

5. Means for remediation and external enforcement.

The organisation should establish a privacy policy that includes a means to address harm[14] to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.

The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organisation and enhance its reputation for complying with its policies and meeting its obligations to individuals.

Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organisation should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organisation recognise and respond to the legal authority exercising proper jurisdiction.

Public Policy Issues

While many aspects of the essential elements are already well established in law, self-regulation and corporate practices, consideration of several issues could usefully assist and stimulate the robust adoption of an accountability approach. These include the following:

[14] The concept of harm can include, among other things, compromise of an individual's financial or physical well-being; embarrassment; and damage to reputation. Additional work is needed to more clearly define and describe harm as it can result from violation of privacy and inappropriate use of data.

1. **How does accountability work in currently existing legal regimes?**

   Adopting an accountability approach to global information privacy governance may require reinterpretation or amendment of existing laws to enable the use of accountability mechanisms and to make it easier and more practicable to hold organisations accountable.[15]

   It may, for example, be necessary to provide in law or regulation that organisations comply with requests to inspect or review certain privacy practices to determine whether the organisation meets the essential elements of accountability as discussed in this paper. Work may be required to provide for legal recognition of the internal rules and policies organisations adopt and the measures organisations take to be accountable.[16]

2. **What is the role of third-party accountability agents?**

   Third-party review of an organisation's practices against appropriate criteria will greatly facilitate the success of an accountability approach. Qualified, authorised accountability agents will be an important element to address resource constraints in order to make the accountability approach work in practice.

   Establishing criteria for organisations that wish to serve as accountability agents, and articulating their role and the extent of their authority, will be a key task for policymakers. It will also be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

   Finally, to be useful to organisations, the services of an accountability agent must be affordable from a financial and operations perspective. Accountability agents must be able to price their services in a manner that allows them to recover their cost and build working capital, but still ensure that services are affordable to the full range of organisations that wish to avail themselves of their resources. Certification processes should be meaningful and trustworthy.

---

[15] In its 2008 report the Australian Law Reform Commission considered the possibility that Australian law be amended to assure an accountability approach could be used to improve governance of cross-border data transfers. A number of EU countries are exploring whether amending the law could better accommodate binding corporate rules.

[16] Such amendments are suggested in the APEC Privacy Framework, which requires that organisations comply with local data protection rules, but those amendments must enable them to write cross-border privacy rules that link to the APEC Principles to govern data transfers. Paragraph 46 of the Framework commentary encourages member economies to "endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with applicable laws".

They should also be designed to limit their disruption of business operations and to safeguard the confidentiality of an organisation's data assets.

3. How do regulators and accountability agents measure accountability?

An accountability approach does not rely on a breach to prompt review of an organisation's information practices and protections. Accountability agents and regulators must be empowered to review organisations' internal processes in a manner that allows them to ensure meaningful oversight. Policymakers may also wish to consider the measures to be taken by organisations to test for accountability and to be sure that it is working.

While an organisation's corporate policies must be linked to external criteria in the various countries where it does business, laws may differ from jurisdiction to jurisdiction. Accountability oversight must assess an organisation's overall privacy programme and allow for resolution of those differences in company policies in a manner that furthers the intent of a range of often conflicting laws or regulations.

Policymakers need to identify a way to measure confidence in an organisation's overall privacy accountability programme — commitment, policies and performance mechanisms — to determine whether an organisation is accountable even if its policies and practices are not a one-to-one match for local law and regulation.

4. How is the credibility of enforcement bodies and third-party accountability programmes established?

Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. Assessing accountability requires examining and judging an organisation's entire programme — a somewhat subjective analysis — so that the credibility of accountability agents is critical.[17]

Third-party accountability programmes such as seal programmes may supplement the work of government agencies. The credibility of these third parties must also be established if they are to be trusted by privacy enforcement agencies and the public. Investment in robust process and experienced, thoughtful staff will be essential to their success.

Additional work should be undertaken to determine how the credibility of these organisations is tested. It will be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the

[17] Work already undertaken at the OECD may be helpful in this regard. See Organisation for Economic Co-operation and Development, *Recommendations on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007).

criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

5. **What are the special considerations that apply to small- and medium-sized enterprises that wish to demonstrate accountability, and how can they be addressed?**

   In many cases, organisations that wish to demonstrate accountability may be small- and medium-sized enterprises, ("SMEs") for which privacy protection resources may be limited. Consideration must be given to the special needs of these organisations and the impact that fulfilling the essential element may have on these enterprises. It may be that aspects of the essential elements will need to be tailored or adapted for smaller organisations in a manner that makes them more workable but does not dilute them.

   Assessment requirements provide one example. While assessments may well serve the same function for SMEs as they do for larger organisations, such assessments may pose an undue burden on smaller enterprises with scarce resources. The nature of the assessment and the parties that may carry them out may differ for such entities, depending on the nature and sensitivity of the data in question. It will be important to examine how an SME might fulfill the assessment requirement without compromising itself financially. Similar questions of scalability as they apply to these organisations will need to be considered and resolved.

Conclusion

Dramatic advances in the speed, volume and complexity of data flows across national borders challenge existing models of data protection. In the face of such complexity and rapid change, data protection must be robust, yet flexible. Privacy can no longer be guaranteed either through privacy notices and consent opportunities for individuals, or through direct regulatory oversight.

An accountability-based approach to data protection helps to address these concerns. It requires that organisations that collect, process or otherwise use personal information take responsibility for its protection and appropriate use beyond mere legal requirements, and that they be accountable for any misuse of the information that is in their care.

Accountability does not redefine privacy, nor does it replace existing law or regulation. While mechanisms to achieve privacy goals will remain the concern of both policymakers and organisations, an accountability approach shifts the focus of privacy governance to an organisation's ability to achieve fundamental data protection goals and to demonstrate that capability.

While there is already a greater focus on accountability in recent data protection enactments and discussion, and much can be accomplished within existing frameworks,

there is also a growing awareness that organisations that use personal data need to put in place and ensure compliance with the five essential elements of accountability:

(1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria;

(2) Mechanisms to put privacy policies into effect, including tools, training and education;

(3) Systems for internal, ongoing oversight and assurance reviews and external verification;

(4) Transparency and mechanisms for individual participation; and

(5) Means for remediation and external enforcement.

The path forward is clear, if at times daunting. The promise of an accountability-based approach to international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates alike — robust transfer and use of data in a fashion that is responsible and that ensures meaningful protections for individuals. To realise this goal, policymakers and the leaders of organisations must undertake the challenging and necessary work towards greater emphasis on true accountability.

Appendix
Galway Project Participants

The following lists the participants in the Galway Project. This list indicates participation in the Galway Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Marcus Belke, 2B Advice

Bojana Bellamy, Accenture

Daniel Burton, Salesforce.com

Emma Butler, Information Commissioner's Office, United Kingdom

Fred Cate, Indiana University, Maurer School of Law

Maureen Cooney, TRUSTe

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Peter Hustinx, European Data Protection Supervisor

Takayuki Kato, Consumer Affairs Agency, Japan

Christopher Kuner, The Centre for Information Policy Leadership, Hunton & Williams LLP

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Data Protection Commissioner, Spain

Rocco Panetta, Panetta & Associates

Daniel Pradelles, Hewlett Packard Company

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Scott Taylor, Hewlett Packard Company

Bridget Treacy, The Centre for Information Policy Leadership, Hunton & Williams LLP

K. Krasnow Waterman, Massachusetts Institute of Technology

Armgard von Reden, IBM Corporation

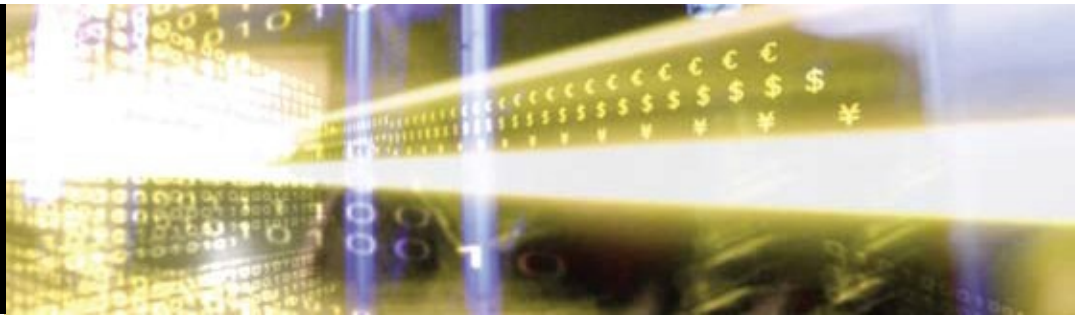
Jonathan Weeks, Intel Corporation

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



Demonstrating and Measuring Accountability
A Discussion Document

Accountability Phase II – The Paris Project

October 2010

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Paris Project

Preface

Martin E. Abrams
Centre for Information Policy Leadership

When the participants in the Accountability Project released its discussion paper on accountability's essential elements in October 2009, they did so recognizing that within the framework described in that document, it would be necessary to address questions about the its real-world implementation The Centre for Information Policy Leadership at Hunton & Williams LLP was pleased to facilitate further work on accountability, assembling experts to consider practical questions: How do organisations demonstrate their accountability? How do regulators measure it?

This document proposes fundamental conditions that accountable organizations should be prepared to implement and demonstrate to regulators. It further considers how and under what circumstances organisations would measure accountability. Participants recognized that accountability could not be a one-size-fits-all approach. For accountability to work, both organisations and regulators must be able to implement and measure fundamentals in a way that is appropriate for the organization, its business model, and the way that it collects, uses and stores data. When accountability is demonstrated and measured may depend in some cases upon the risks to individuals an organisation's activities raise.

In discussions and in the writing of this paper, participants recognized an increased focus on accountability in national and international discussions about improved data governance. Since October 2009, the principle of accountability has featured prominently in the "The Future of Privacy," released by the Article 29 Working Party in December 2009, The Opinion of the Article 29 Working Party released in July 2010, and the global data protection standards of the Madrid Resolution. It is hoped that this paper reflects the participants' awareness of this growing body of work.

An accountability approach requires organizations to establish policies consistent with recognized external criteria. One universally accepted set of guidance would enhance accountability's potential to bridge various national and regional legal regimes. The Madrid Resolution, adopted by the International Conference of Data Protection and Privacy Commissioners in October 2009, is an important first step toward realizing that vision and deserves close consideration.

Looking ahead, we are pleased that the Spanish Data Protection Authority has agreed to facilitate next year's meetings. That phase of the work will likely consider what will be required of accountability agents, how and when organisations will validate their accountability, and incentives for organisations to attain different degrees of accountability.

This paper has benefited from the insights and perspectives of all sectors – industry, civil society, academia, and government.[1] The Centre is particularly encouraged by the participation of data protection commissioners and privacy regulators from Canada, France, Germany, Hungary, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, the United Kingdom and the United States, as well as the European Data Protection Supervisor. Their active involvement highlights the significance and timeliness of this effort.

The Centre would like to thank the CNIL for graciously facilitating the March and June meetings and for providing us with critique and counsel, and all of the experts who thoughtfully and generously contributed to the discussions in Paris and to the drafting of this paper. While their participation has been critical to the success of the work, the Centre alone is responsible for any errors.

[1] The members of the group of experts are listed in the Appendix.

Demonstrating and Measuring Accountability
The Accountability Project – Phase II
Paris, France

Introduction

Over the past 18 months, policymakers around the world have undertaken efforts to examine and update privacy protections in a way that better serves the needs of individuals and organisations[1] and takes into account the realities of technologies and data flows of the 21st century. The concept of accountability has figured prominently in many of these discussions.

An accountability principle has been a feature of both the earliest of the major international instruments on privacy, the Organisation for Economic Cooperation and Development's Privacy Guidelines, published in 1980,[2] and the most recent, the Asia Pacific Economic Cooperation's APEC Privacy Framework, endorsed in 2005.[3] Both require that organisations "should be accountable for complying with measures that give effect" to the fair information practices articulated in the respective guidelines.

New approaches to privacy protection currently under consideration rely significantly on accountability as a means to ensure protection of data. The joint paper of the European Union Article 29 Data Protection Working Party (Article 29 WP) and the Working Party on Police and Justice (WPPJ), "The Future of Privacy,"[4] notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalisation and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability."[5] In a later Opinion on accountability submitted to advise the European Commission on how to amend the Data Protection Directive, the Article 29 WP defined a statutory accountability principle to "explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request."[6]

The APEC Privacy Framework depends upon an organisation's implementation of fair information practices, particularly accountability, to facilitate protected cross-border data flows. Discussions held during the recent series of Federal Trade Commission Roundtables entitled "Exploring Privacy" repeatedly identified accountability as an approach to data governance in a world of increasingly complex data uses and flows. And the proposed international data protection standards of the Madrid Resolution include accountability, stating that responsible persons should take all necessary measures to observe the obligations set forth in the resolution and put in place the mechanisms necessary to demonstrate such observance to individuals and supervisory authorities.[7]

For purposes of this project, accountability can be described as a *demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data.*

---

[1] This document uses the term organisation generally. An accountability approach may apply to public and private sector bodies including – but not limited to – for-profit organisations, non-governmental organisations, educational and cultural institutions, and government and law enforcement agencies.

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited 10 May 2010).

[3] http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf (last visited 29 July 2010).

[4] "The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," 02356/09/EN WP 168, December 1, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

[5] Commissioner Peter Hustinx, speaking at the European Data Protection Conference on 29 April 2010, said, "the principle of accountability in our contribution was. .. intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice."

[6] Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN - WP 173, para. 5. http://www.cbpweb.nl/downloads_int/wp173_en.pdf.

[7] "Internacional Standards on the Protection of Personal Data and Privacy: The Madrid Resolution," released October 2009, http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf (last visited 30 July 2010).

In 2009, Phase I of the Accountability Project (Galway) articulated a set of essential elements of accountability. It is against these elements that an organisation's accountability would be established. They are as follows:

(1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria.

(2) Mechanisms to put privacy policies into effect, including tools, training and education.

(3) Systems for internal, ongoing oversight and assurance reviews and external verification.

(4) Transparency and mechanisms for individual participation.

(5) Means for remediation and external enforcement.[8]

In Phase I, [9] participants recognized that for the approach to work in practice, it would be necessary to resolve practical, implementation-oriented questions, such as how organisations demonstrate accountability, and how regulators measure it. These questions were the subject of Phase II of the Accountability Project which convened in Paris in March and June 2010. At those meetings, experts considered the objectives of accountability, and began to formulate a set of common fundamentals to be demonstrated and measured.

This paper is the result of the discussions at the Paris meetings and of extensive comment and review by participants. While this document does not answer all outstanding questions, it does consider in practical terms how accountability may be measured and demonstrated. Participants in Phase II – international experts from government, industry, academia, and civil society – recognized the importance of framing the practices related to demonstrating and measuring accountability as accurately as possible to avoid unnecessary burdens or unintended consequences that could inadvertently stifle innovation or adoption of new, beneficial technologies.[10]

Approaches to accountability include both regulatory and voluntary components. This paper addresses concepts, principles, methodologies and techniques that could apply across legal frameworks and cultural orientations. Discussions related to accountability have reflected consensus about the need to allow organisations, the flexibility to develop, consistent with recognized external criteria, appropriate practices, and regulatory authorities similar flexibility to adapt compliance reviews and methods to the organisation under review. Thus, even in regulated environments, accountability schemes may first emerge as voluntary mechanisms that enable a "race to the top." Early adopters would demonstrate the hallmarks of accountability in measureable ways. As the confidence of regulators and others in the concept of accountability increases, especially if early adopters take a responsible and constructive approach, it can be widely expected that others will follow. In due course, accountability could become a major and widely-used means of achieving practical effectiveness without imposing unnecessary burdens.

The Scope of Accountability and Benefits to Organisations

A General Requirement of Accountability

When its work began in early 2009, an important goal of the Accountability Project was to develop an approach to privacy and data governance that would facilitate cross-border transfers of data. The project sought to establish the conditions necessary to certify organisations as accountable for the exchange of data with entities outside of their jurisdiction. Such an approach would create a trusted environment in which regulators would have high confidence that organisations would continue to comply with data protection requirements when processing outside their jurisdictions, and would address problems once identified.

As the Accountability Project's work progressed, the principle of accountability became the subject of discussions in other forums considering improvements to existing data protection regimes. In particular, accountability figures prominently in the European Commission's consultation on the legal framework for data protection. The Article 29 WP and the WPPJ in December 2009 issued a joint contribution to the consultation that identified challenges to the current EU legal framework for data protection and the Commission's opportunity to introduce accountability as an innovative response. In July 2010,

[8] "Data Protection Accountability: The Essential Elements - A Document for Discussion," October 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last visited, 30 July 2010).

[9] In Phase I, the Accountability Project began a series of discussions about accountability, particularly as an improved approach to governing trans-border data flows. The Project assembled a group of international experts from government, industry and academia to consider how an accountability-based system might be designed. The experts defined the essential elements of accountability, examined issues raised by the adoption of the approach, and proposed additional work required to facilitate establishment of accountability as a practical and credible mechanism for information governance.

[10] Participants in Phase II of the Accountability Project are listed in the Appendix.

the Article 29 WP issued Opinion 3/2010 on the principle of accountability, proposing that accountability "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request." The opinion considered accountability in light of both global movement of data and EU framework as a "way of encouraging data controllers to implement practical tools for effective data protection."[11]

This proposed application of accountability to all aspects of data governance prompted the Accountability Project to consider how accountability might serve the full range of data protection functions within organisations, of which the transfer of data across borders represents only one.

Such broad implementation suggests that, as a starting point, all data controllers should be required to meet a level of accountability that provides fundamental assurances. Some controllers, however, may be motivated by stated incentives, and may choose to demonstrate various degrees or kinds of accountability. It may be that certain kinds of accountability, with specific or more rigorous standards, will facilitate proof of the organisation's readiness to engage in certain activities (such as international data transfers) or to be relieved of certain administrative burdens that may be established in regulation (such as notification or registration requirements).

The Accountability Project anticipates several benefits for multiple stakeholders that could result when organisations fulfill a general requirement of accountability. Organisations that can demonstrate adherence to and implementation of accountable practices encourage a data environment where the confidence and trust of individuals is enhanced. Organisations would be better positioned to re-allocate scarce resources to activities that encourage optimal privacy protection for individuals and away from fulfilling requirements (such as re-notification of minor changes in processing) that are costly but that may provide little added protection for data in practice. Were organisations as a general rule to meet the requirements of accountability, data protection authorities' resources could be redirected away from more *pro forma* administrative activities and toward addressing irresponsible actors in the marketplace.

A Customized Approach

This paper proposes a set of common fundamentals that an organisation will need to demonstrate to establish their accountability. These nine fundamentals are designed to provide guidance. Accountability is not a "one-size-fits-all" approach, however, and all organisations will need to determine, consistent with recognized external criteria, which of these nine and/or others they will implement. The fundamentals should be applied in a way that is appropriate to the organisation's business model, data holdings, technologies and applications, and the risks to privacy they raise for individuals. For example, an organisation with highly sensitive data that regularly employs the services of third party processors may need to fulfill a set of fundamentals different from those adopted by an organisation holding less sensitive data. Each organisation would be required to make thoughtful decisions about the fundamentals it needs to implement to demonstrate its accountability.

Paragraph 41 of the Article 29 WP Opinion proposes its own set of common accountability measures.[12] The measures set forth are not intended to represent a comprehensive list. But perhaps more importantly, it is welcome that the document does not anticipate that all measures will necessarily apply to all organisations in every circumstance. It also envisions that the general legal obligation to adopt accountability measures is supported by a proposed "toolbox" of measures for data controllers that would provide guidance about what could constitute, depending on the circumstances, the appropriate measures to be adopted by the data controller. What measures are appropriate would be decided on a case-by-case basis by the organisation, resulting in custom-built solutions, whereby controllers tailor measures to the specifics of their data holdings and their systems.

[11] Legislation introduced before the United States Congress also includes provisions requiring corporate accountability for privacy protections.

[12] The Article 29 Working Party proposed a set of "common accountability measures" that might include: 1. Establishment of internal procedures prior to the creation of new data processing operations (internal review, assessment, etc.); 2. Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc.), which should be available to data subjects; 3. Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations; 4. Appointment of a data protection officer and other individuals with responsibility for data protection; 5. Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.; 6. Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects; 7. Establishment of an internal complaint handling mechanism; 8. Setting up internal procedures for the effective management and reporting of security breaches; 9. Performance of privacy impact assessments in specific circumstances; 10. Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc.). Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN - WP 173, Paragraph 41.

The Role of Certification - Review and Acceptance of Practices

For purposes of accountability, certification of an organisation's practices involves review and acceptance by the appropriate supervisory authority or accountability agent. The general requirement to be accountable does not carry with it an obligation to be certified by a third party. However, organisations that wish to engage in certain activities or accrue certain benefits may be required to obtain certification. For example, an organisation may wish to engage in transfer of data outside of its home jurisdiction, or be relieved of certain administrative burdens imposed by regulation. To attain such benefits, organisations may be required to obtain some level of certification. Doing so may involve submitting to a consultation with the certifying authority, which could specify certain fundamentals that the organisation must demonstrate.

It is anticipated that evaluation of organisations by a certifying authority would also be conducted on a case-by-case basis. As stated earlier, one size does not fit all, and certifying authorities will need to determine which of the common fundamentals of accountability an organisation will need to demonstrate.

Binding Corporate Rules (BCRs) provide a good example in principle, though not yet in practice, of how certification of accountability can provide benefits to individuals. BCRs require that organisations demonstrate that they are compliant and will remain compliant with requirements defined by EU data protection authorities for transferring data outside of the EU. When organisations enter into BCRs they are relieved of the pre-approval requirement for specified cross-border data transfer, giving them greater flexibility.

When certification would be required, what a certification process might entail, what benefits to organisations might flow from certification, and how to design a certification process that is cost effective and efficient for both regulators and organisations are all issues that remain to be considered.

Demonstrating Accountability

For What Are Organisations Accountable?

Any discussion about what organisations should demonstrate to establish their accountability raises the question: for what are organisations accountable?

- *Existing law and regulation* - Organisations are accountable for complying with applicable law and regulations.
- *Private sector oversight programs* - Organisations that sign on to a self-regulatory program meet the requirements of that program and submit to its oversight and enforcement in order to be deemed accountable.
- *Privacy promises* - Accountable organisations fufill the promises stated in their privacy policies.
- *Ongoing risk assessment and mitigation* - Accountable organisations assess and understand the risks that collection, use, processing and retention of data pose to individuals, and take steps to address those risks.[13] In an environment in which the nature of data collection, analysis, and use changes rapidly, law, regulation and guidance often lag behind new developments. Within accountable organisations, risk assessment and mitigation keeps pace with changes in technology, applications, business models, personnel, and the commercial and political climate in a way that more traditional means of protection often may not. It also aligns with evolving societal or cultural norms.

To Whom Are Organisations Accountable?

Organisations may be accountable to three entities: data subjects/individuals, regulators, and business partners.

- *Individuals* - Individuals expect their data to be secured, and to be used and managed responsibly. They require that organisations handle their data in a manner consistent with the requirements of law, regulation, and the organisation's posted privacy policy.
- *Regulators* - Privacy and data protection regulators require that organisations comply with applicable law and regulation, and that they honor the commitments they make to individuals regarding the collection, use, and management of their information.

[13] "Data Protection Accountability: A Document for Discussion," October 2009, http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (last visited 10 May 2010).

→ *Business Partners* - Accountable organisations also answer to business partners. While contracts and legal obligations apply, vendors need adequate information about the nature of the data and the obligations attendant to it, and assurances that the accountable data owner has complied with any requirements with respect to that data and its sharing with the vendor. Accountable users of outside vendors need assurances that these obligations can be met by their business partners no matter where the vendor may process the data.

Common Fundamentals of an Accountability Implementation Program

Participants in the Accountability Project identified nine common fundamentals that an accountable organisation should implement. Organisations that wish to be deemed accountable should be cognizant of the fundamentals, and prepared to demonstrate their fulfillment of these conditions as appropriate to the nature of the data they collect, their busniess model, and the risks their use of data raises for individuals.

1. Policies: *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.*

An organisation should develop, implement and communicate to individuals data privacy policies informed by appropriate external criteria found in law, regulation, or industry best practices, and designed to provide the individual with effective privacy protections. The organisation should also design and deploy procedures to put those policies into effect in light of the specific circumstances of its own organisations (e.g., what is collected, how it is used, and how systems and organisations are connected).

2. Executive Oversight: Internal executive oversight and responsibility for data privacy and protection.

Executive oversight will require the creation of a data privacy leader supported by appropriate resources and personnel, and responsible for reporting to organisation leadership. Commitment by top management should include appropriate reporting and oversight of the organisation's privacy program. Top management should empower and require senior-level executives to develop and implement the organisation's programs, policies and practices. Small and medium-sized organisations will need to allocate oversight resources appropriately, keeping in mind the extent and sensitivity of its data holdings and the nature of the use of the data.

3. Staffing and Delegation: *Allocation of resources to ensure that the organisation's privacy program is appropriately staffed by adequately trained personnel.*

While recognizing the need to work within economic and resource constraints, accountable organisations should have in place sufficient staff to ensure the success of their privacy program. Such staff should receive adequate training, both as they assume their role in the privacy program and as that program evolves to address new developments in the organisation's business model, data collection practices and technologies, and offerings to consumers. Delegation of authority and responsibility for data protection to appropriate units or parts of the organisation has been found to be effective in many accountable organisations. Many accountable organisations have found that situating the responsibility for privacy locally and throughout the organisation has resulted in optimal resource placement and awareness. As in the case of oversight, staffing and delegation decisions in small and medium-sized organisations should reflect the particular circumstances of the organisation and its activities, and the nature, size and sensitivity of its data holdings.

4. Education and awareness: *Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations.*

Organisations should provide the necessary briefings, information and education for their personnel to keep them apprised of current and emerging requirements. Such education should involve keeping employees aware of new data protection issues that may affect the performance of their job, and sensitive to the importance of data privacy to individuals and to the success and reputation of the organisation.

5. Ongoing risk assessment and mitigation: *Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks.*

To be accountable, organisations must assess the risks to privacy raised by their products and practices as they are developed, implemented and evolve, and as their data requirements change. In response to the findings of those assessments, organisations must take measures to mitigate those risks. Risk assessment is not static, but an ongoing function that responds to the dynamic, evolving nature of data collection, use and processing.

Privacy Impact Assessments are one important risk assessment and mitigation tool. A Privacy Impact Assessment is carried out as part of the process for determining whether to collect data, deploy a new technology or data-driven business model, or use or manage data in a particular way. It is also important when making decisions about how best to secure data. It involves close examination of each new application or process, an evaluation of its attendant risks, and a determination of the steps that must be taken to ensure that the manner in which data is used meets the requirements of applicable law, regulation and the organisation's privacy promises.

To be accountable for its risk assessment and mitigation practices, organisations also should be able to demonstrate the nature of their risk analysis. The organisation must show the rigor of the criteria against which analyses are carried out, and the suitability of those criteria to the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are made and steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective.

6. Program risk assessment oversight and validation: *Periodic review of the totality of the accountability program to determine whether modification is necessary.*

An accountable organisation should periodically review its privacy and data protection accountability program to ensure that it continues to meet the needs of the organisation by supporting sound decisions about data management and protection that promote successful privacy outcomes.

To encourage transparency, the results of that program review should be available to those persons or organisations external to the reviewing group tasked with program oversight. The method by which this information is derived and reviewed must be both appropriately rigorous and cost effective for both organisations and regulators. The results of these assessment measures and/or audits should be reported to the appropriate personnel within the organisation, and when necessary, corrective action should be taken.

7. Event management and complaint handling: *Procedures for responding to inquiries, complaints and data protection breaches.*

An accountable organisation should implement a well-designed, reliable procedure for addressing data protection problems when they arise. Such procedures will need to effectively address data protection problems, such as data misuse, misappropriation or breach. They also must include a formal complaint procedure to address concerns of individuals regarding data protection practices, and potential or actual failures, and to ensure that the rights of individuals related to their data are respected.

8. Internal enforcement: *Internal enforcement of the organisation's policies and discipline for non-compliance.*

Accountable organisations should have in place policies and procedures for enforcement of internal data protection rules. Personnel who disregard those rules or misappropriate or misuse data are subject to sanctions, including dismissal.

9. Redress: *The method by which an organisation provides remedies for those whose privacy has been put at risk.*

Accountable organisations should establish redress mechanisms whereby individuals may have their complaints heard and resolved. The redress mechanisms should be appropriate to the character of the organisation, the nature of its data holdings, and the way the data is used and appropriate for the specific issue. The redress mechanism should be readily and easily accessible by individual, and address complaints efficiently and effectively. Industry groups may offer options for individual organisations seeking to implement a redress mechanism. As the specific attributes of an appropriate redress may vary from culture to culture and from industry to industry, decisions about redress will likely be local. Guidance about redress would optimally be developed in consultation with experts, regulators, civil society, and representatives of public and private sector organisations.

Measuring Accountability

Although measurement may not always be required, accountable organisations should be prepared to demonstrate their programs when asked. For example, under Canadian law,[14] while every organisation is required to be accountable, not every organisation will undergo accountability review. However, even when measurement is not required, accountable organisations should be prepared to demonstrate on an ad hoc basis how they safeguard personal data.

[14] Canada's Personal Information Protection and Electronic Documents Act provides that every organisation must be accountable for its compliance with the requirements of the Act. It does not as a matter of course, however, require review of an organisation's compliance.

When an organisation wishes to demonstrate its accountability to enable it to engage in certain activities, make certain assertions, or be relieved of certain regulatory requirements, more formal review and measurement by a supervisory authority or a third-party accountability agent recognized by the supervisory authority may be required. In such cases, supervisory authorities or third-party accountability agents will be responsible for evaluating and measuring an organisation's compliance with applicable regulations and in some cases its privacy promises. They will also measure accountability based on the organisation's demonstration of policies, privacy programs, and assurance processes.

Such organisations must thus be able to provide evidence of the programs they have implemented to ensure that privacy/data protection principles are put into effect. The evidence may be reviewed at the request of the supervisory authority or as part of a review by a third-party recognized accountability agent. Depending on legal requirements, supervisory authorities may be able to request such evidence proactively or in the course of an evaluation or investigation. Again, consistent with applicable legal frameworks, supervisory authorities may recognize third-party accountability to undertake this role.

Finally, resolution of complaints, spot checks and enforcement will be important to the credibility of an accountability approach. When recognized by supervisory authorities, third-party accountability agents can assume an important role in carrying out these functions, alleviating the burden on authorities with scarce resources.

The Accountability Project identified the following stages in the measurement of an organisation's accountability program. These may or may not occur sequentially, but represent an ongoing process of education, risk assessment, self-certification, review and enforcement.

1. The organisation takes appropriate measures to establish processes and procedures that implement its privacy policies. It carries out risk analysis and mitigation based on their understanding of its obligations under an accountability approach. The organisation may enlist the consultation of the supervisory authority or recognized accountability agent in this process and complete the appropriate documentation.

2. The organisation self-certifies that it meets the requirements of accountability.

3. The supervisory authority or recognized accountability agent reviews such filings and provides some form of acceptance of the certification.

4. The organisation submits to enforcement by the supervisory authority or recognized accountability agent. The supervisory authority or accountability agent will hear and resolve complaints from individuals. It will also conduct appropriate organisation spot checks to ensure that they continue to meet the criteria to which they have self-certified.[15]

5. Supervisory authorities, recognized accountability agents, trade associations, and government agencies engage in raising the awareness of organisations about the obligations that an accountable organisation must meet, and the benefits that flow from being accountable.

Questions about when measurement should take place are yet to be resolved. When should organisations submit to evaluation? When review is necessary, should it occur at the time an accountability program is implemented? Or is it effective and efficient to allow organisations to self-certify their accountability and open themselves to spot checks and review when a significant data protection problem arises or breach occurs?[16] These questions also arise depending upon the scope of an organisation's accountability. Should the timing and requirements of measurement differ if an organisation seeks accountability certification for cross-border data sharing, or for accountable data practices generally?[17]

Issues for Resolution

1. How will remediation work in an accountability approach?

For an accountability approach to have credibility, it must include a mechanism by which complaints are heard and addressed. Policymakers will need to explore and establish effective remediation mechanisms that will reflect and serve the

[15] The manner in which spot-checks might be conducted, and the criteria by which the decision whether to carry out such a review might be determined, requires further consideration. When developing a policy related to such reviews, it will be important to consider the burdens to organisations, the need for defined processes and regulator expectations, and strategic approaches that direct oversight toward where the risks are greatest.

[16] The question of whether ex-ante or ex-post review is appropriate to measure accountability has been the subject of significant discussion. It may be that review prior to or after implementation of an accountability program will depend upon the degree or level of accountability an organisation wishes to achieve. For example, an organisation wishing to attain certification for the highest level of accountability may submit to review before their program is operational. Some data protection authorities (i.e., Canadian), however, rely primarily on ex-post assessment by means of a complaint process.

[17] In many ways, these questions relate to the issue of validation, which this paper identifies as a question for consideration in future work.

requirements of national culture, regulation, self-regulation and law. In cases where industry sectors, regulatory authorities or non-governmental organisations have already established complaint and investigation redress processes, organisations and policymakers may wish to use them as a foundation for the development of remediation mechanisms that specifically serve an accountability approach. Such efforts are already underway as part of the re-examination of the EU data protection directive,[18] the review of the Australian privacy law,[19] and the notice of inquiry issued by the Department of Commerce in early 2010, "Information Privacy and Innovation in the Internet Economy."[20] Organisations will also need to correct or improve processes or procedures that have been shown to be inadequate as a result of a complaint investigation, findings of a validation procedure or data breach.

2. How do organisations determine the appropriate validation mechanism?

Validation by appropriate parties that organisations are in fact implementing the necessary processes and procedures will be important to the effectiveness and credibility of an accountability approach. Validation is distinct from certification; validation rather is a step in the certification process that establishes confidence that policies, implementation mechanisms, and assurance processes are in place and working. The objectives of validation include testing the existence of program elements, assessing the appropriateness of the accountability program's coverage throughout the organisation, and ensuring that the policies and processes are effective. Costs of validation vary based on what is being tested.

Validation takes many forms and carries different meaning in different countries and within different industries. Terms such as audit, internal audit, specialized negative audits and assurance reviews – all of which refer to forms of validation – have different meanings in different industries and locations. Extensive discussions will be required to fully understand the various validation options, the applicability of those options in an accountability program, and the kind of validation necessary to establish confidence in an organisation's accountability program.

Participants in the accountability meetings in Paris reviewed validation mechanisms and requirements that ranged from the most procedurally demanding (e.g., binding corporate rules) to approaches like that taken in Canadian law which require accountability but make no provision for validation.

In Paris participants did not, however, decide what level of validation is appropriate. Making this determination will require evaluating costs, the nature of the data in question, the manner in which the data is to be used and possible legal requirements. Additional exploration is needed to better understand the factors involved in identifying the right validation method, and policymakers will need to make that determination.

3. On what basis are third-party accountability agents recognized?

Third-party accountability agents may play a role in measuring accountability. Accountability agents can be recognized and charged with certifying that the organisation's risk analysis is sound and its program is capable of maintaining effective accountability processes. They may also be accredited to evaluate and approve organisations' applications to be certified as accountable. Accountability agents may play a role in resolution of complaints, spot checks and enforcement.

Third-party review of an organisation's practices against appropriate criteria will greatly facilitate the success of an accountability approach. Qualified, recognized accountability agents will be an important to addressing resource constraints.

Policymakers will need to establish criteria for organisations that wish to serve as accountability agents, and to articulate their role and the extent of their authority. Policymakers will also need to develop criteria by which the credibility and trustworthiness of third party accountability agents can be judged. In establishing this guidance, it will be important that policymakers are mindful that the services of accountability agents must be priced to allow them to develop and sustain a viable business, but still ensure that services are affordable to organizations with less funding as well as those with deeper resources.

Ideally, policy related to the role and operation of third-party accountability agents will be developed in consultation with those organisations, business users, government representatives, experts and civil society.

[18] Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN, WP173.

[19] "Australian Privacy Principles: Exposure Draft," http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/exposure_draft.pdf (last visited 30 July 2010). This review of privacy principles is one part of a broader inquiry into information privacy protection law in Australia.

[20] http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf (last visited 9 September 2010).

Conclusion

Accountability has assumed increased prominence in international and national discussions about data protection regimes. Phase II of the Accountability Project builds upon the essential elements to articulate practical guidance about how accountability may be demonstrated by organisations and measured by regulators. It envisions a general requirement of accountability that will be met by all organisations and that will benefit organisations, regulators and individuals. While organisations would not, as a general rule, be reviewed by regulators or their recognized accountability bodies, every organisation would be required to stand ready to demonstrate its accountability. For organisations that wish to engage in activities that may raise heightened risk to individuals, certification may be necessary.

To be deemed accountable, organisations will need to demonstrate and regulators will measure certain fundamentals. Accountability is a customized approach, so that what those fundamentals are will depend upon the nature of the organisation, its data holdings, and the risk its activities raise for individuals. The fundamentals include:

(1) Policies

(2) Executive oversight

(3) Staffing and delegation

(4) Education and awareness

(5) Ongoing risk assessment and mitigation

(6) Program risk assessment oversight and validation

(7) Event management and complaint handling

(8) Internal enforcement

(9) Redress

Exploration of how these fundamentals will be validated and certified, how third party accountability agents will be recognized is still necessary.

The need for an accountability-based approach to international privacy protection to ensure robust transfer and use of information in a manner that minimizes risks to individuals and ensures meaningful protection – continues to grow. Identifying and understanding the practical means necessary to implement accountability will be key to its successful adoption. While additional issues require resolution, understanding the way in which organisations demonstrate, and regulators measure accountability is an important step toward that goal.

Appendix

Accountability Project Phase II – The Paris Project Participants

The following lists the participants in the Accountability Phase II – The Paris Project. This list indicates participation in the Paris Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Amit Ashkenazi, Law Information and Technology Authority, Israel

Carman Baggaley, Office of the Privacy Commissioner, Canada

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Emmanuelle Bartoli, CNIL

Bojana Bellamy, Accenture

Emma Butler, Information Commissioner's Office, United Kingdom

Daniel Burton, Salesforce.com

Fred H. Cate, Indiana University, Maurer School of Law

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Leigh Feldman, Bank of America

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Peter Fleischer, Google

Anne-Marije Fontein-Bijnsdorp, Data Protection Authority, The Netherlands

Christine Frye, Bank of America

Jose Leandro Nunez Garcia, Data Protection Agency, Spain

Jose Manuel de Frutos Gomez, European Commisssion

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Yoram Hacohen, Head, Law Information and Technology Authority, Israel

Silke Harz, Office of the Federal Data Protection Commissioner, Germany

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Sandy Hughes, Procter & Gamble Company

Peter Hustinx, European Data Protection Supervisor

The Honorable Michael Kirby

Christopher Kuner, The Centre for Information Policy Leadership, Hunton & Williams

Laraine Laudati, European Commission

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Director, Data Protection Agency, Spain

Brendon Lynch, Microsoft Corporation

Fran Maier, TRUSTe

Olivier Matter, CNIL

Madeleine McLaggan, Commissioner, Data Protection Authority, The Netherlands

Daniel Pradelles, Hewlett-Packard Company

Olivier Proust, Hunton & Williams

Krisztina Rajos, Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary

Kathryn Ratte, United States Federal Trade Commission

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Sachiko Scheuing, Acxiom

Russell Schrader, Visa Inc.

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Blair Stewart, Office of the Privacy Commissioner, New Zealand

Jennifer Stoddart, Privacy Commissioner, Canada

Scott Taylor, Hewlett-Packard Company

Omer Tene, College of Management School of Law, Israel

K. Krasnow Waterman, Massachusetts Institute of Technology

Nigel Waters, Privacy International

Jonathan Weeks, Intel Corporation

Yael Weinman, United States Federal Trade Commission

Boris Wojtan, Accenture

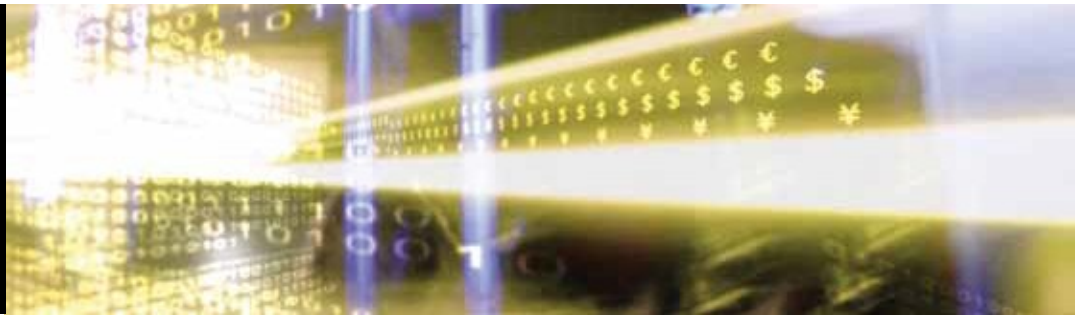
Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

Richard Thomas, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



Implementing Accountability in the Marketplace
A Discussion Document

Accountability Phase III - The Madrid Project
November 2011

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Madrid Project

Preface

Martin E. Abrams
Centre for Information Policy Leadership

Since its work began in 2009, the Accountability Project has described an innovative, 21st century approach to data protection. Accountability builds on traditional notions of fair information practices, but incorporates new elements that require organisations to implement comprehensive privacy programmes and base their decisions about data on credible assessment of the risks they raise for individuals and how best to mitigate them. It has articulated the conditions that must exist in an accountable organisation – conditions that organisations must be able to demonstrate and that regulators can measure.

Over the last three years, accountability has figured prominently in data protection policy development around the world. In the European Union, the work of the Article 29 Working Party referenced accountability in its submission to the Commission's consultation on changes to the Directive, and issued an opinion on accountability. Accountability has been reflected in policy instruments issued in the United States, and data protection agencies in Canada have embarked on a project to define their expectations of accountable companies. In Mexico, new data protection laws and regulations incorporate accountability. At the Asia Pacific Economic Cooperation forum, work is underway to design a mechanism based on accountability that would bridge approaches to data protection taken in different countries. In response to these advances in public policy, many companies have taken important steps toward implementing an accountability programme.

This year, the Project responded to suggestions in public policy discussions that accountability, in order to be effective, must be required across the marketplace. Participants considered what would be required of organisations in such circumstances, and what benefits the approach would offer as a result of such broad implementation. They further explored the requirements and benefits of accountability when formally recognised by a third party.

While this progress is encouraging, a great deal of work remains if accountabiity is to serve as an effective solution for data protection and privacy. Data protection authorities and agencies, organisations and third-party accountability agents will need to implement programmes and procedures to support accountability, and the practical aspects of how that infrastructure might work requires further exploration. Questions remain about how organisations will establish the validity of the statements they provide to demonstrate their accountability. More work is also needed to determine the nature of the relationship between data protection authorities necessary to resolve cross-border privacy issues, and to better understand the appropriate role and level of authority of third-party accountability agents. As the Project has considered accountability in greater detail, reaching consensus on all issues has become more challenging.The document references areas where differences remain and additional work is necessary.

The Centre for Information Policy Leadership at Hunton & Williams has been privileged to serve as secretariat for the Project, and developed this paper to document the third year of its work. As in past years, the Project has benefited from an international group of experts from business, government, data protection and regulatory agencies, and the advocacy community. The Centre is particularly grateful and encouraged by the active participation of data protection commissioners and privacy regulators from Canada, France, Germany, Hungary, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, the United Kingdom and the United States, as well as the European Data Protection Supervisor. Their active and ongoing involvement highlights the global concern about this issue.

The Centre would like to thank the Spanish Data Protection Agency for graciously facilitating the February and June meetings in Madrid, and the United States Federal Trade Commission for hosting the meeting held in Washington, DC, in March. Their insights and counsel as we planned meetings and drafted this document were invaluable to the success of this year's work. We thank all of the experts for their thoughtful contributions to the discussions and for their generous review and critique of this document. While Centre staff developed this document, the paper reflects the work of many people who contributed ideas and kindly reviewed drafts. However, it does not necessarily reflect the views of any participant, and the Centre alone is responsible for any errors that may remain.

Executive Summary

The Accountability Project entered its third year aware of the growing understanding, both within the Project and in public policy discussions, that to be most effective, an accountability approach to data protection should be explicitly required across the marketplace.

If all organisations were required to be accountable, all would implement privacy programmes proportional to the size, sensitivity and complexity of their data holdings and business models. Such broad application of accountability promises benefits to individuals, the market, and organisations. While the principles of accountability would apply to all organisations, their implementation would be custom designed – tailored to the size, sensitivity and complexity of their data holdings, their business models, and applicable law and regulation.

Accountable organisations will share several common characteristics. All accountable organisations will:

- Adopt privacy policies consistent with commonly accepted external criteria – applicable law, regulation, and recognised guidelines;
- Implement mechanisms to put those policies into effect and communicate them to individuals;
- Integrate privacy protections into corporate governance;
- Put in place an internal oversight programme; and
- Be prepared to demonstrate to a regulator its commitment to accountability and its capacity to provide necessary data and privacy protections by providing evidence, when asked, that it has implemented each of the elements described above.

Broad application of accountability promises benefits to individuals, the market, and organisations. Accountability is envisioned to:

- Heighten the confidence of individuals and organisations that their data will be protected regardless of where or by whom it is stored or processed;
- Lead to higher levels of compliance;
- Enhance data protection efficiency by allowing regulators to focus their resources on activities that raise the greatest risk to individuals;
- Improve the quality of data protection by allowing organisations to use and update tools that best respond to specific risks;
- Better position regulators to police the marketplace against activities that fall outside law, regulation and guidance through more efficient resource allocation;
- Create an expectation in the marketplace that organisations will act in accordance with the requirements of accountability; and
- Bridge data protection regimes across jurisdictions, allowing countries and regions to pursue common data protection objectives through different but equally reliable means.

While all organisations would be required to be accountable, in certain cases, when they wish to enjoy enhanced benefits or engage in certain activities, organisations might choose to take additional steps to establish their status as having attained *recognised accountability.* Recognised accountability requires that an organisation meet all of the requirements, as articulated in the essential elements, for accountability. It must also take additional steps to provide evidence and documentation that it has fulfilled the essential elements *before* status as recognised is granted. An organisation seeking recognised accountability would be required to provide:

- A description of its internal privacy and data protection policies, and evidence that those policies have been approved by the appropriate authority within the organisation;
- A description and evidence of the programmes it has put in place to implement its policies;
- A description of the manner in which it has incorporated privacy and data protection into its corporate governance, and measures or metrics by which the success of its incorporation can be assessed; and

- A description of the procedures it has implemented to oversee the effectiveness of its privacy and data protection programme, including metrics related to monitoring.

An organisation that is recognised as accountable would be expected to enjoy the following benefits:

- Relief from certain administrative regulatory requirements or administrative burdens;
- Appropriate consideration of recognised status in the context of an enforcement action;
- A consultative relationship with third-party accountability agents that allows for appropriate remediation processes/opportunities prior to enforcement actions;
- Recognition of the integrity of programme design by the appropriate supervisory authority; and
- Competitive advantage by signaling to the market its enhanced commitment to privacy and data protection.

Every organisation, whether or not it has been recognised as accountable, will be subject to oversight by a regulatory authority and/or its appointed accredited agent. The reasons for which an authority may initiate an inquiry, and the showings required in response are as follows:

As part of a random check of accountability. An accountable organisation will be required to provide a description of its:

- Internal policies based on external criteria;
- Programme that implements its internal policies;
- Integration of its privacy protection programme into overall organisation governance; and
- Privacy and data protection oversight programme.

Pursuant to an investigation of a suspected or actual privacy or data protection failure. An organisation will be required to provide:

- A description of its internal policies linked to external criteria as they apply to the area of the enterprise under investigation;
- A description of its programme implementing its privacy policies, and evidence that the programme has been implemented;
- Evidence of how it has integrated privacy and data protection into corporate governance, and meaningful metrics to demonstrate the extent of such integration; and
- A description of its oversight programme as it applies to the data activities under investigation, and metrics about that monitoring.

As follow-up to an enforcement action. An organisation will be required not only to provide evidence of its privacy and oversight programmes (as in the case of an investigation of a suspected privacy or data protection failure, above), but also to have those aspects of its privacy initiative validated by a third party.

Introduction

Since 2009, the Accountability Project ("the Project") has engaged in an ongoing discussion about an approach to data and privacy protection that would take into account the rapid pace of technology innovation; ubiquitous collection, analysis and processing of data; powerful analytics; and global flows of information that support the information economy. The Project recognised that in this data environment, organisations must deploy effective programmes to protect individuals against the risks that the use of information may create. While individuals must continue to play an appropriate role in making choices about the use and sharing of data pertaining to them, choice must be meaningful, taking into account complex technologies, business models and data uses. At the same time, organisations need to be able to process and analyse data in creative, innovative ways that enable them to respond quickly to customer and marketplace requirements.

The Project has described *accountability* as an approach that requires companies to implement programmes that foster compliance with data protection principles and to be able to explain how those programmes provide the required protections for individuals. Accountability obligates organisations to take responsibility for the safe and appropriate processing and storage of data, wherever it occurs. It requires them to implement effective data and privacy protection policies that correspond to accepted external criteria found in law, regulation and industry best practices. Accountability asks that organisations analyze

and understand the risks that data use raises for individuals, and take necessary and appropriate steps to mitigate those risks. It further requires that organisations make judicious decisions about data use, even when traditional individual consent or choice may not be available.

The accountability principle is not new. It is a feature of both the earliest of the major international instruments on privacy, the Organisation for Economic Cooperation and Development's Privacy Guidelines,[1] published in 1980, and the most recent, the Asia Pacific Economic Cooperation's Privacy Framework,[2] endorsed in 2004. Both state that organisations "should be accountable for complying with measures that give effect" to the fair information practices articulated in the respective guidelines. It is also the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),[3] and has traditionally played a role in implementation of privacy processes in the European Union.[4]

New approaches currently under consideration significantly rely on accountability as a means to ensure the protection of data. "The Future of Privacy,"[5] the joint paper of the European Union Article 29 Data Protection Working Party and the Working Party on Police and Justice, notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalization and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability." In a later Opinion on accountability[6] submitted to advise the European Commission about how to amend the Data Protection Directive, the Article 29 Working Party defined a statutory accountability principle to "explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request."

This document is the third in a series of papers issued by the Accountability Project. The first, released in October 2009,[7] articulated the essential elements that an organisation must adopt in order to be accountable.[8] It stated that an accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to promote responsible decisions about the management and protection of data. Such external criteria include applicable law, regulation, and recognised external guidelines. The paper further stated that accountability requires that organisations design and implement comprehensive data and privacy protection programmes[9] based on analysis of the risks data use raises for individuals and on responsible decisions about how those risks can be appropriately mitigated.

The second paper, issued by the Project in October 2010,[10] examined how organisations demonstrate accountability and how regulators measure it. The paper proposed fundamental conditions that accountable organisations should be prepared to establish and demonstrate to regulators.[11] It further considered how, and under what circumstances, regulators, data protection authorities, and their designated agents would measure accountability. The paper noted that accountability is not a one-size-fits-all approach: both organisations and regulators must be able to implement and measure the fundamentals in a manner suitable for the organisation, its business model, and the way it collects, uses and stores data.

---

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html.

[2] APEC Privacy Framework, http://www.ag.gov.au/www/agd/rwpattach.sf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[3] This governance was explicitly described in a 2009 publication of the Office of the Privacy Commissioner of Canada, "Processing Personal Data Across Borders: Guidelines." http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm. In PIPEDA, accountability is an overarching principle that applies to protection and management of data, whether it is maintained and processed domestically or transferred outside Canadian borders for storage and processing.

[4] Paragraph 19 of the Article 29 WP "Opinion 3/2010 on the principle of accountability" (adopted on 13 July 2010, 00062/10/EN, WP 173) cites Binding Corporate Rules used in the context of international data transfers as reflecting the accountability principle. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[5] http://www.garanteprivacy.it/garante/document?ID=1707337.

[6] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[7] "Data Protection Accountability: The Essential Elements - A Document for Discussion," October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

[8] The essential elements articulated by the Accountability Project are: 1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria; 2) Mechanisms to put privacy policies into effect, including tools, training and education; 3) Systems for internal, ongoing oversight and assurance reviews and external verification; 4) Transparency and mechanisms for individual participation; 5) Means for remediation and external enforcement. The essential elements are described in more detail in Appendix A.

[9] The essential elements of accountability require that such programmes be designed to implement privacy policies linked to established external criteria.

[10] "Demonstrating and Measuring Accountability: A Discussion Document," http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.pdf.

[11] The Accountability Project identified nine common fundamentals that an accountable organisation should implement: 1) Policies; 2) Executive Oversight; 3) Staffing and Delegation; 4) Education and awareness; 5) Ongoing risk assessment and mitigation; 6) Program risk assessment oversight and validation; 7) Event management and complaint handling; 8) Internal enforcement; 9) Redress. The fundamentals are described in detail in Appendix B.

The discussions of this second phase of the work on accountability reflected a growing appreciation that for an accountability approach to data protection to be most effective, accountability should be explicitly required across the marketplace. All organisations would be required to implement privacy programmes proportional to the size, sensitivity and complexity of their data holdings and business models. Such broad application of accountability promises benefits to individuals, the market, and organisations. In certain cases, however, when they wish to enjoy enhanced benefits or engage in certain activities, organisations might choose to be formally recognised as accountable. In such instances, organisations would likely take additional steps to establish their status as having attained recognised accountability.

In 2011, the Centre for Information Policy Leadership, through a process facilitated by the Spanish Data Commissioner, convened the third international discussion about the architecture and implementation of an accountability approach to data governance – this time to focus on questions pertaining to what is required of accountable organisations, and what additional steps are required of organisations that wish to be recognised as accountable. Participants considered these issues at three meetings, held in Madrid and Washington, DC. They discussed the benefits that would accrue to the marketplace, individuals, regulators and organisations as a result of broad implementation of an accountability requirement. They also articulated what would be required of organisations seeking to attain *recognised accountability*, and the discrete, specifically identifiable benefits they would enjoy.

Participants in this phase of the Project – international experts from government, regulatory agencies, industry, academia and civil society – identified a drafting committee that oversaw Centre staff as they prepared this document, which was circulated later for comment among all participants. This paper is the result of that process.

Accountability Applied Across the Marketplace

Requirements

Accountability is built upon the essential elements described in the paper issued by the Project in 2009.[12] Accountable organisations establish data and privacy-protection policies consistent with commonly accepted external criteria and deploy programmes to carry out those policies. They rely on identification and mitigation of risks to individuals as the basis for their judgment about which measures will best protect data.

While the principles of accountability would apply to all organisations, their implementation would be custom-designed. Organisations will tailor their privacy programmes to their business model; the nature and size of their data holdings; the technologies and applications they deploy; and the risks data and its applications pose to the rights and freedoms of individuals. One size does not fit all, and the rigor, breadth and detail of an organisation's privacy programme will correspond to the risks to the rights and freedoms of individuals raised by data and its applications, as assessed by the organisation. While certain fundamentals may be found in data protection programmes, all measures will not necessarily apply to all organisations in every instance.[13] Moreover, the privacy programme may vary across an organisation. Some aspects of the organisation may process large quantities of sensitive data; others may deal only with non-sensitive information. The organisation also may implement different programmes to address the privacy risks raised by use of different kinds of data.

All programmes, however, would share several common characteristics.[14] First, accountable organisations would adopt privacy policies consistent with commonly accepted external criteria – applicable law, regulation, and recognised external guidelines. Such policies would also reflect the organisation's values and promises it has made to individuals.[15]

Second, accountable organisations would implement mechanisms to put policies into effect and communicate those policies to individuals. Mechanisms would include processes to assess, manage and mitigate the privacy risks created by data use; employee training; and the means to manage data events such as breach, inappropriate access, or failure to meet the obligations of the privacy policy.

Third, accountable organisations would integrate privacy protections into governance and apply them across all aspects of the organisation where they are relevant. Their policies would enjoy the support and commitment of executive management.

[12] See fn. 6 and Appendix A.

[13] The fundamentals proposed by the Accountability Project would serve as a toolbox for organisations as they develop their privacy programmes. In its "Opinion 3/2010 on the principle of accountability," the Article 29 Working Party suggests a similar approach, and offers an example of such a custom-designed programme. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. Actual programmes will be designed appropriate to the nature of the organisation and its enterprise, as discussed elsewhere in this paper.

[14] In some jurisdictions, the specifics of an organisation's implementation of accountability mechanisms will be reflected in binding contracts.

[15] Ideally, an organisation's privacy policies will be consistent with policies it implements to address other risks, *e.g.,* security risks, and overarching policies of the business.

The organisations would designate a person or persons at an appropriately senior level to be responsible for privacy and data protection initiatives throughout the organisation.[16] Such person or persons would be provided sufficient staffing and resources to effectively implement the organisation's privacy and data protection policies.

Fourth, accountable organisations would put in place an internal oversight programme. Accountability requires effective oversight of the privacy programme by the individual or team responsible for privacy, and an internal monitoring and assessment process to assure that it fosters sound decisions about data use and effective protections. In addition, accountable organisations would oversee and raise awareness of third-party vendors and suppliers with whom they do business to ensure that they are meeting the obligations created by law, regulation and the organisation's privacy promises to its customers.

Finally, organisations adhering to requirements of accountability would be prepared to demonstrate to a regulator their commitment to accountability and their capacity to provide necessary data and privacy protections. They would do so by providing evidence, when asked, that they have implemented each of the elements described above.[17]

In many cases, organisations would design and build programmes to address their specific situation. This may especially be the case for large, complex and well-established companies that are deeply familiar with the data protection issues confronting their enterprise and the marketplace. In other instances (particularly for small- and medium-sized enterprises), industry associations may develop and offer models for privacy programmes that companies may tailor to their needs. In every instance, however, programmes that meet the requirements of general accountability would adopt privacy policies linked to commonly-accepted external criteria, programmes and processes to put those policies into effect, internal oversight and assurance review to determine whether privacy programmes are effective, and metrics that enable the organisation to demonstrate their accountability when asked to do so.

Benefits of Accountability Adopted Across the Marketplace

When required across the marketplace, accountability promises benefits to individuals, businesses, the market and regulators. Accountability is expected to:

- Heighten the confidence of individuals and organisations that their data will be protected wherever and by whomever it is stored or processed;
- Lead to higher levels of compliance by explicitly requiring organisations to implement comprehensive programmes that put into effect data protection principles, and to stand ready to demonstrate the capacity of those programmes to foster responsible use, management and protection of data;
- Enhance data protection efficiency by allowing regulators to focus their resources, oversight and enforcement on those activities that create the most risk for individuals;
- Help organisations improve the quality of data protection by allowing them to use tools that best respond to specific risks, and to rapidly update those tools to quickly meet the requirements of new business models and emerging technologies;
- Better position regulators to police marketplace participants whose activities fall outside the bounds of law, regulation and recognised guidance, by enabling them to direct limited resources toward organisations that have not established their accountability or that fail to comply;
- Create an expectation in the marketplace – for business partners, commercial vendors and individuals – that organisations will operate in accordance with the requirements of general accountability, that will drive organisations toward accountable practices; and
- Bridge data protection regimes across jurisdictions, by allowing countries and regions to pursue common data protection objectives through different but equally reliable means.

Recognised Accountability

While all organisations will be required to be accountable, in some cases, organisations may choose to take steps to be *recognised* as accountable.

[16] An organisation will designate a senior person or persons responsible for privacy and data protection as appropriate to the structure of the organisation.

[17] What an accountable organisation must show is discussed in detail in the section, "Responding to Official Oversight," of this document.

An organisation may adopt or deploy a new technology, application, or process, and may wish to be recognised as doing so in an accountable manner. It may wish to seek recognition for business or competitive reasons. It may wish to transfer data across borders for business processing, and want recognition that it has engaged in the appropriate risk assessment and mitigation and is implementing appropriate protections. In these and other cases, an organisation may seek recognised accountability.

Benefits to Organisations

While general adoption of accountability yields benefits to organisations, regulators, the market and individuals, companies that take the initiative to attain recognised accountability must realise discrete, identifiable benefits over and above these. Organisations will need to make investments – sometimes significant – to attain and maintain recognised accountability, and will need to experience recognisable advantages to justify the additional costs incurred.

It is envisioned that organisations that are recognised as accountable would enjoy certain benefits, including:

- Relief from certain administrative regulatory requirements or administrative burdens (*e.g.,* approval to transfer data across borders, model contracts, individual notification requirements);[18]
- Appropriate consideration of recognised status in the context of an enforcement action;
- A consultative relationship with third-party accountability agents that allows for an appropriate remediation process/opportunity prior to an enforcement action;
- Recognition of the integrity of programme design by the appropriate supervisory authority; and[19]
- Competitive advantage, by signaling to the market the organisation's enhanced commitment to privacy and data protection.

Requirements

Recognised accountability requires that an organisation meet all of the requirements for general accountability, based on the essential elements and as described above.

In addition to fulfilling the requirements of accountability, an organisation seeking recognition would be required to provide evidence and documentation of its fulfillment of the essential elements.[20] An organisation seeking recognised accountability would be required to provide:

- A description of its internal privacy and data protection policies, and evidence that those policies have been approved by the appropriate authority within the organisation;
- A description and evidence of the programmes it has put in place to implement its policies;
- A description of the manner in which it has incorporated privacy and data protection into its governance, and measures or metrics by which the success of its incorporation can be assessed;[21] and
- A description of the procedures the organisation has implemented to oversee the effectiveness of its privacy and data protection programme, including metrics related to monitoring.[22] The organisation could also provide evidence of the review of the oversight mechanism through validation by an independent auditor, regulator or third party agent.[23]

[18] Relief from administrative regulatory requirements would only be possible insofar as it is provided for by law.

[19] Not all data protection and privacy laws currently in place are sufficiently flexible to enable organisations that attain recognised accountability to enjoy these benefits.

[20] Some data protection authorities participating in the Project believe that recognition of an organisation as accountable must involve the data protection authority and occur before any benefits take effect. Others believe that self certification is possible and believe that third party accountability agents can provide the necessary assurances so that an organisation can enjoy benefits of recognised accountability. This question requires further exploration by this Project.

[21] Such metrics could include by whom and at what level in the organisation the privacy strategy and programme is reviewed; and where and at what level within the organization hierarchy the person responsible for privacy is placed.

[22] Such metrics of monitoring could include statistics about how often certain activities are reviewed; how often the organisation assesses the efficacy of its programme; an assessment of the quality of the decisions it yields; and how frequently the organisation revisits its risk assessment and mitigation strategy, particularly when new products and services are offered.

[23] European Binding Corporate Rules require that organisations and data protection authorities come to agreement about common binding references that define what is expected of organisations.

Such validation may be carried out by an independent party within the organisation, or by a third party validation agent.[24]

Type of Accountability	Internal Policies	Implementation Programme	Privacy Governance	Oversight
Accountability				
All companies would	- Develop internal policies based on external criteria - Be prepared to provide evidence of approval by appropriate internal authority	- Implement the policies - Be prepared to provide evidence of implementation	- Develop a governance programme - Be prepared to provide evidence of governance	- Develop an internal oversight programme - Be prepared to provide evidence of internal monitoring and review
Recognised Accountability				
Companies seeking and demonstrating recognised status from regulator or third-party agent would	- Provide description of internal policies based on external criteria - Provide evidence of approval by appropriate internal authority	- Provide description of implementation programme - Provide evidence of implementation	- Provide description of governance programme - Provide metrics related to governance	- Provide description of oversight programme - Provide metrics related to monitoring - Provide evidence of review by independent auditor, regulator or third party agent

Responding to Official Oversight

Every organisation, whether or not it has been recognised as accountable, will be subject to oversight by a regulatory authority and/or their appointed accredited agent. Such authorities may initiate an inquiry for a number of reasons.

Authorities may initiate an inquiry about an organisation's accountability as part of a *random check of accountability*. In such cases, organisations will be required to provide a description of its implementation of the four elements of accountability – its internal policies based on external criteria; privacy and data protection programme; integration of its privacy protection programme into overall corporate governance; and privacy and data protection oversight programme.

Authorities also may initiate an inquiry *pursuant to an investigation of a suspected or actual privacy or data protection failure*. In response to such an inquiry, organisations can be expected to be required to provide a number of things relative to the area of enterprise under investigation.

An organisation could be asked to describe its internal policies linked to external criteria, as they apply to the area of the enterprise under investigation. It may be required to provide not only a description of its programme implementing its privacy policies, but also evidence that the programme has, in fact, been implemented. The organisation may provide evidence of how it has integrated privacy and data protection into corporate governance, and provide meaningful, reliable metrics to demonstrate the extent of such integration. Such metrics could, for example, include the organisation's budget for the privacy function, the number of staff dedicated to privacy, evidence of product reviews conducted, and the number of training sessions

[24] When validation for accountability is required, it must be cost-effective for both privacy protection regulators and agencies, and the companies that seek recognition. To be optimally effective, validation methods must be recognised across the marketplace. The validation system an organisation uses must be appropriate to the nature of the organisation, its data holdings and applications, and its business model. While no validation system is foolproof, it must be sufficiently rigorous to raise the level of trust within the market that organisations have met the requirements necessary for validated accountability. Questions related to the sufficiency of different types of validation methods will be taken up in year four of the Project.

carried out for employees. However, metrics may vary depending on the nature of the organisation, the data it collects and maintains, and the risks raised by its use.

An organisation could also be asked to provide a description of its oversight programme as it applies to the data activities under investigation, and metrics about that monitoring, including how frequently the privacy team reviews data processes within business units, how often specialized security audits are carried out; and the number of business unit or process internal audits.

Finally, in *cases where a failure has in fact been identified*, the organisation could be required not only to provide evidence of its privacy and oversight programmes, but to have these aspects of its privacy initiative validated by a third party.

Officials may initiate an inquiry as a follow-up to an investigation and enforcement action, to ensure that required remediation has been carried out. Such inquiries may involve periodic independent audit of the organisation in areas that are the subject of the investigation and enforcement action.

Responding to an Official Inquiry	Internal Policies	Implementation Programme	Privacy Governance	Oversight
Organisations responding to a random accountability check would	- Provide description of internal policies based on external criteria	- Provide description of implementation programme	- Provide description of governance programme	- Provide description of oversight programme
Organisations responding to an investigation of suspected failure or resulting from evidence of actual failure would	- Provide description of internal policies based on external criteria relative to area in question	- Provide description of implementation programme relative to area in question - Provide evidence of implementation - When finding of failure, validation by a third party is required.	- Provide description of governance programme relative to area in question - Provide metrics related to governance	- Provide description of oversight programme relative to area in question - Provide metrics related to monitoring - When finding of failure, validation by a third party is required.
Organisations responding to an enforcement follow-up would				- Provide results of periodic independent audit of area in question

Conclusion

The practical success of an accountability approach will rely significantly on its broad implementation across the marketplace. When all organisations implement the essential elements, benefits accrue to individuals, the marketplace, and organisations themselves – greater confidence in data protection, better compliance, efficiencies for regulators and organisations, and a heightened expectation on the part of individuals and the market that organisations will act in accordance with the requirements of accountability. Recognised accountability offers enhanced benefits to organisations that may wish to transfer data across borders, adopt a new technology or business model, or simply signal their heightened attention to accountable practices.

Accountability continues to figure prominently in discussions about data protection and privacy within countries and in international forums. Going forward, the Project will focus in a more detailed way on the infrastructure necessary for successful implementation of an accountability approach by organisations and by regulators. While some of the mechanisms that will make up this infrastructure may require action by policymakers before they can be realised, it is important that the work begin.

APPENDIX A

The Essential Elements of Accountability[25]

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.

An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices.

An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by tasking appropriate staff with implementing the policies and overseeing those activities.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

3. Systems for internal ongoing oversight and assurance reviews and external verification.

Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle – from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful – and must be subject to some form of monitoring

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.

The organisation should also periodically engage – or be engaged by – the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution.

4. Transparency and mechanisms for individual participation.

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

[25] Excerpted from "Data Protection Accountability: The Essential Elements," October, 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also provides for those instances when it is feasible. In such cases, it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

5. Means for remediation and external enforcement.

The organisation should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.

The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution.

APPENDIX B

Common Fundamentals of an Accountability Implementation Programme[26]

Participants in the Accountability Project identified nine common fundamentals that an accountable organisation should implement. Organisations that wish to be deemed accountable should be cognizant of the fundamentals, and prepared to demonstrate their fulfillment of these conditions as appropriate to the nature of the data they collect, their business model, and the risks their use of data raises for individuals.

1. ***Policies:*** *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.*

An organisation should develop, implement and communicate to individuals data privacy policies informed by appropriate external criteria found in law, regulation, or industry best practices, and designed to provide the individual with effective privacy protections. The organisation should also design and deploy procedures to put those policies into effect in light of the specific circumstances of its own organisations (e.g., what is collected, how it is used, and how systems and organisations are connected).

2. ***Executive Oversight:*** *Internal executive oversight and responsibility for data privacy and protection.*

Executive oversight will require the creation of a data privacy leader supported by appropriate resources and personnel, and responsible for reporting to organisation leadership. Commitment by top management should include appropriate reporting and oversight of the organisation's privacy programme. Top management should empower and require senior-level executives to develop and implement the organisation's programmes, policies and practices. Small and medium-sized organisations will need to allocate oversight resources appropriately, keeping in mind the extent and sensitivity of its data holdings and the nature of the use of the data.

3. ***Staffing and Delegation:*** *Allocation of resources to ensure that the organisation's privacy programme is appropriately staffed by adequately trained personnel.*

While recognizing the need to work within economic and resource constraints, accountable organisations should have in place sufficient staff to ensure the success of their privacy programme. Such staff should receive adequate training, both as they assume their role in the privacy programme and as that programme evolves to address new developments in the organisation's business model, data collection practices and technologies, and offerings to consumers. Delegation of authority and responsibility for data protection to appropriate units or parts of the organisation has been found to be effective in many accountable organisations. Staffing and delegation decisions in small and medium-sized organisations should reflect the particular circumstances of the organisation and its activities, and the nature, size and sensitivity of its data holdings.

[26] Excerpted from "Demonstrating and Measuring Accountability: A Discussion Document," http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.pdf.

4. ***Education and awareness:*** *Existence of up-to-date education and awareness programmes to keep employees and on-site contractors aware of data protection obligations.*

Organisations should provide the necessary briefings, information and education for their personnel to keep them apprised of current and emerging requirements. Such education should involve keeping employees aware of new data protection issues that may affect the performance of their job, and sensitive to the importance of data privacy to individuals and to the success and reputation of the organisation.

5. ***Ongoing risk assessment and mitigation:*** *Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks.*

To be accountable, organisations must assess the risks to privacy raised by their products and practices as they are developed, implemented and evolve, and as their data requirements change. In response to the findings of those assessments, organisations must take measures to mitigate those risks. Risk assessment is not static, but an ongoing function that responds to the dynamic, evolving nature of data collection, use and processing.

To be accountable for its risk assessment and mitigation practices, organisations also should be able to demonstrate the nature of their risk analysis. The organisation must show the rigor of the criteria against which analyses are carried out, and the suitability of those criteria to the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are made and steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective.

6. ***Programme risk assessment oversight and validation:*** *Periodic review of the totality of the accountability programme to determine whether modification is necessary.*

An accountable organisation should periodically review its privacy and data protection accountability programme to ensure that it continues to meet the needs of the organisation by supporting sound decisions about data management and protection that promote successful privacy outcomes. To encourage transparency, the results of that programme review should be available to those persons or organisations external to the reviewing group tasked with programme oversight. The method by which this information is derived and reviewed must be both appropriately rigorous and cost effective for both organisations and regulators. The results of these assessment measures and/or audits should be reported to the appropriate personnel within the organisation, and when necessary, corrective action should be taken.

7. ***Event management and complaint handling****: Procedures for responding to inquiries, complaints and data protection breaches.*

An accountable organisation should implement a well-designed, reliable procedure for addressing data protection problems when they arise. Such procedures will need to effectively address data protection problems, such as data misuse, misappropriation or breach. They also must include a formal complaint procedure to address concerns of individuals regarding data protection practices, and potential or actual failures, and to ensure that the rights of individuals related to their data are respected.

8. ***Internal enforcement:*** *Internal enforcement of the organisation's policies and discipline for non-compliance.*

Accountable organisations should have in place policies and procedures for enforcement of internal data protection rules. Personnel who disregard those rules or misappropriate or misuse data are subject to sanctions, including dismissal.

9. ***Redress:*** *The method by which an organisation provides remedies for those whose privacy has been put at risk.*

Accountable organisations should establish redress mechanisms whereby individuals may have their complaints heard and resolved. The redress mechanisms should be appropriate to the character of the organisation, the nature of its data holdings, and the way the data is used and appropriate for the specific issue. The redress mechanism should be readily and easily accessible by individual, and address complaints efficiently and effectively. Industry groups may offer options for individual organisations seeking to implement a redress mechanism. As the specific attributes of an appropriate redress may vary from culture to culture and from industry to industry, decisions about redress will likely be local. Guidance about redress would optimally be developed in consultation with experts, regulators, civil society, and representatives of public and private sector organisations.

Accountability Phase III - The Madrid Project Participants

The following lists the participants in the Accountability Phase III - The Madrid Project. This list indicates participation in the Madrid Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Brendan Van Alsenoy, Interdisciplinary Centre for Law and ICT, Belgium

Carman Baggaley, Office of the Privacy Commissioner, Canada

Andrea Krisztina Bárányos, Office of the Parliamentary Commissioner for Data Potection and Freedom of Information, Hungary

Rosa Barcelo, Office of the European Data Protection Supervisor

Christophe Begot, Total, S.A.

Bojana Bellamy, Accenture

Emma Butler, Information Commissioner's Office, United Kingdom

Giovanni Buttarelli, Office of the European Data Protection Supervisor, Belgium

Fred H. Cate, Indiana University, Maurer School of Law

Peter Cullen, Microsoft Corporation

Susan Daley, Symantec Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Stephen Deadman, Vodafone

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Leigh Feldman, Bank of America

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Peter Fleischer, Google

Christine Frye, Bank of America

Jose Leandro Nunez Garcia, Data Protection Agency, Spain

Carlos García-Mauriño, Oracle

Jennifer Barrett Glasgow, Acxiom Corporation

Rafael Garcia Gozalo, Data Protection Agency, Spain

Constance Graham, Procter & Gamble Company

Silke Harz, Office of the Federal Data Protection Commissioner, Germany

Billy Hawkes, Data Protection Commissioner, Ireland

Markus Heyder, United States Federal Trade Commission

David Hoffman, Intel Corporation

Sandy Hughes, Procter & Gamble Company

Brian Huseman, Intel Corporation

Barbara Lawler, Intuit, Inc.

Brendon Lynch, Microsoft Corporation

Jean-Guy Mahaud, Total, S.A.

Fran Maier, TRUSTe

Maria Marvan, Federal Institute for Access to Information and Data Protection, Mexico

Georgina Nelson, Which?, London

Mikko Niva, Nokia

Daniel Pradelles, Hewlett-Packard Company

Artemi Rallo, Agencia Española de Protección de Datos, Spain

Kostas Rossoglou, BEUC - The European Consumers' Organisation, Belgium

Russell Schrader, Visa Inc.

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Scott Taylor, Hewlett-Packard Company

Adriana Lopez-Tafall, Merck & Co., Inc.

Bridget Treacy, Hunton & Williams LLP

Hilary Wandall, Merck & Co., Inc.

Jonathan Weeks, Intel Corporation

Nigel Waters, Australian Privacy Foundation and Privacy International

Jan-Boris Wojtan, Accenture

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

Richard Thomas, The Centre for Information Policy Leadership, Hunton & Williams LLP