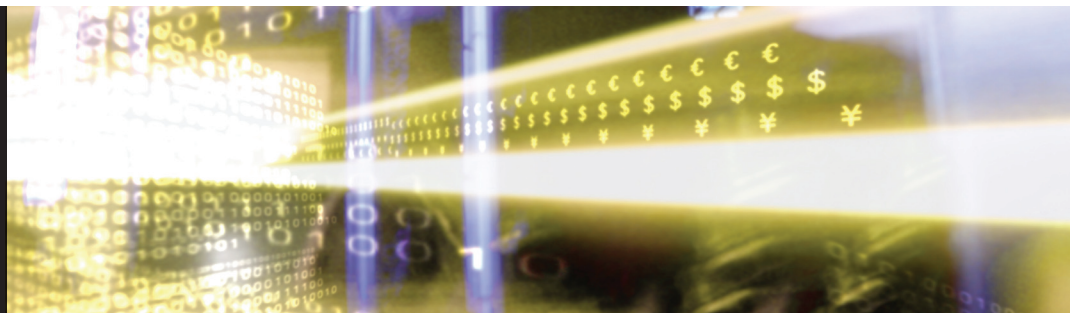


ACCOUNTABILITY: A COMPENDIUM FOR STAKEHOLDERS

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS

TABLE OF CONTENTS

<u>Document</u>	<u>Tab</u>
Data Protection Accountability: The Essential Elements	1
Demonstrating and Measuring Accountability	2
Privacy by Design: Essential for Organizational Accountability and Strong Business Practices	3
<i>Accountability: Part of the International Public Dialogue About Privacy Governance</i> , by Paula J. Bruening (BNA International)	4
<i>Data Tagging for New Information Governance Models</i> , by Paula J. Bruening and K. Krasnow, The IEEE Computer and Reliability Societies	5
“A New Approach to International Transfers,” Centre’s Response to the European Commission’s Communication on a “A comprehensive approach to personal data protection”	6



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 Guidelines²; 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 Rule³ 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 Guidelines⁵ 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 programmes¹³ 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 harm¹⁴ 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

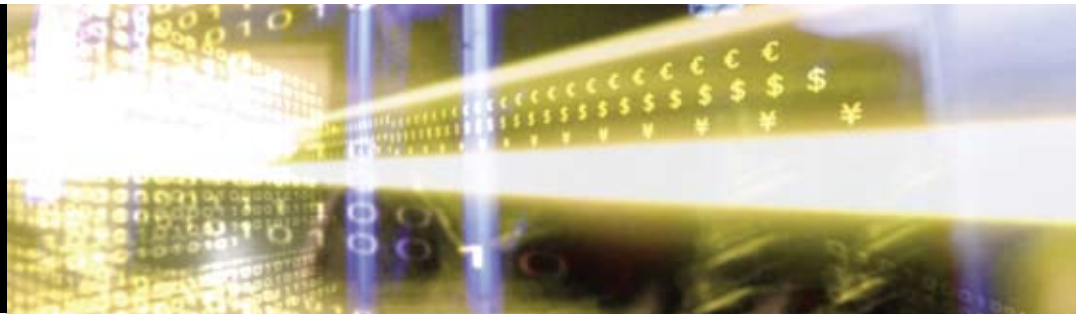
Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams
LLP

THE CENTRE

FOR INFORMATION
POLICY LEADERSHIP

HUNTON & WILLIAMS LLP

© 2009 The Centre for Information Policy Leadership LLP. The content of this paper is strictly the view of the Centre for Information Policy Leadership and does not represent the opinion of either its individual members or Hunton & Williams LLP. The Centre does not provide legal advice. These materials have been prepared for informational purposes only and are not legal advice, nor is this information intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Please do not send us confidential information. Visit us at www.informationpolicycentre.com.



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 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 organisations¹ 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](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.cbppweb.nl/downloads_int/wp173_en.pdf.

⁷ "International 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 fulfill 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 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 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, WP 173.

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/fnotices/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
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

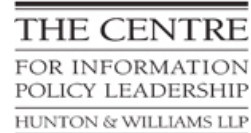
HUNTON & WILLIAMS LLP

© 2010 The Centre for Information Policy Leadership LLP. The content of this paper is strictly the view of the Centre for Information Policy Leadership and does not represent the opinion of either its individual members or Hunton & Williams LLP. The Centre does not provide legal advice. These materials have been prepared for informational purposes only and are not legal advice, nor is this information intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Please do not send us confidential information. Visit us at www.informationpolicycentre.com.

Privacy by Design: Essential for Organizational Accountability and Strong Business Practices



November 2009



Acknowledgements

The authors wish to acknowledge Fred Carter, Senior Policy and Technology Advisor, Policy Department at the Information and Privacy Commissioner's Office, Ontario, Canada for his input on this paper, as well as Susan Smith, Americas Privacy Officer, Hewlett-Packard Company and staff at The Centre for Information and Policy Leadership at Hunton & Williams LLP.

Table of Contents

Foreword	1
I Introduction.....	3
II Convergence of Accountability and <i>Privacy by Design</i>	4
III The Essential Elements of Accountability.....	5
IV <i>Privacy by Design</i> : 7 Foundational Principles.....	6
V Leadership Companies are Demonstrating <i>Privacy by Design</i>	8
<i>Privacy by Design</i> – an HP Example	8
VI Conclusion	14

Foreword

The proposition that “privacy is good for business” is one that is enshrined in all Fair Information Practices (FIPs) around the world and, through them, in the many laws and organizational practices upon which they are based. By setting out universal principles for handling personal data, FIPs seek to ensure the privacy of individuals *and* to promote the free flow of personal data and, through them the growth of commerce.

The enduring confidence of individuals, business partners and regulators in organizations’ data-handling practices is a function of their ability to express the FIPs’ core requirements. These are: to limit collection, use and disclosure of personal data; to involve individuals in the data lifecycle, and to apply appropriate safeguards in a thoroughgoing manner. These requirements, in turn, are premised upon organizational openness and accountability. The ultimate results – which are highly desirable – include enhanced trust, improved efficiencies, greater innovation, and a heightened competitive advantage. Privacy *is* good for business.

But the early FIPs drafters and adopters had in mind large mainframe computers and centralized electronic databases. They could never have imagined how leapfrogging revolutions in sensors, bandwidth, storage, and processing power would converge into our current hyper-connected “Web 2.0” networked world of ubiquitous data availability.

It has become trite to observe that data is the lifeblood of the new economy, but who today can truly grasp how large the arteries are becoming, how they are multiplying, where they may lead, and to what end? Everywhere we see near-exponential growth of data creation, transmission, use and storage, by an ever-expanding universe of actors, somewhere out there in the opaque “cloud.” Most of this data is personally-identifiable. And most of it is now controlled by someone other than the individual himself or herself. Thanks to new information flows, today we enjoy unprecedented and nearly unimaginable new services and benefits, but these have been accompanied by unprecedented and once unimaginable privacy threats and harms. Some say that privacy is effectively dead or dying in the information age. We say that it is not, but it *is* rapidly changing shape.

The need for organizational accountability remains constant – indeed, it has become more urgent today than ever before. What is changing are the *means* by which accountability may be demonstrated, whether to individuals, regulators or to business partners. Beyond policy statements, what is needed now are more innovative and more robust methods for assuring that personal data is, in fact, being managed responsibly.

There are many paths to enhanced accountability and assurance, typically involving a mix of technology, policies and practices, and of law and regulation. More than ever before, a comprehensive and proactive *Privacy by Design* approach to information management is called for – one which assures an end-to-end chain of custody and responsibility right from the very start.

Scott Taylor
Chief Privacy Officer
Hewlett-Packard
Company

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Martin E. Abrams
Senior Policy Advisor and
Executive Director
Centre for Information
Policy Leadership,
Hunton & Williams LLP

I Introduction

Professor Paul A. Schwartz recently wrote:

“Companies are now putting internal policies in place, centered on forward looking rules of information management and training of personnel. Such policies are, at the very least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection.”¹

An accountability-based regulatory structure is one where organizations are charged with societal objectives, such as using information in a manner that maintains individual autonomy and protecting the individual from social, financial and physical harms that might come from the mismanagement of information, while leaving the actual mechanisms for achieving those objectives to the organization. One of the best conceptual models for building in the types of controls suggested by Professor Schwartz is *Privacy by Design*. The best in class companies in Schwartz’s study, “Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment,” are using *Privacy by Design* concepts to build business process that use personal information robustly with clear privacy-protective controls built into every facet of the business process. In other words, *Privacy by Design* and accountability go together in much the same way that innovation and productivity go together.

Accountability is the governance model that is based on organizations taking responsibility for protecting privacy and information security appropriately and protecting individuals from the negative outcomes associated with privacy-protection failures. Accountability was first framed as a privacy principle in the OECD Privacy Guidelines.

The Centre for Information Policy Leadership at Hunton & Williams LLP has recently acted as secretariat for the Galway project that defined the essential elements of accountability.

The conceptual model, *Privacy by Design*, was developed by Ontario Privacy Commissioner Ann Cavoukian in the 1990s to address the development of technologies, but she has since expanded it to include business processes.²

Hewlett Packard is in the midst of implementing an accountability tool built on both accountability principles and the key concepts of *Privacy by Design*. HP’s accountability tool is an example of the trend described by Professor Schwartz.

This paper discusses the essential elements of accountability, *Privacy by Design* principles, and provides an example of a control process that uses the principles to implement the essential elements.

1 “Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment,” Paul A. Schwartz, a working paper by The Privacy Projects, October 2009.

2 “Privacy by Design,” Ann Cavoukian, Ph.D., January 2009.

II *Convergence of Accountability and Privacy by Design*

Accountability as both a basic privacy implementation and enforcement principle dates to the approval of the OECD Privacy Framework in 1980. But it is only today that the privacy community is beginning to understand what is meant by accountability-based privacy governance, and how it impacts the structuring of a privacy program. The growth of Binding Corporate Rules in the European Union, Cross-Border Privacy Rules in APEC, Safe Guard concepts in the United States, and data transfers compliant with the Personal Information and Electronic Documents Act (PIPEDA) in Canada has made clear direction on accountability crucial. The Galway project published a paper called “Data Protection Accountability: The Essential Elements,” in October 2009 that enumerated five essential elements for accountability. The paper was developed with a distinguished group of privacy experts from privacy enforcement agencies, government, academia, civil society and business, and facilitated by the Office of the Irish Data Protection Commissioner, and chaired by the Centre. The essential elements make it clear that accountability comes from privacy protections based on commitment to a program where privacy is built into all business processes.

Over a decade ago Ontario Privacy Commissioner Ann Cavoukian began discussing the virtues of building privacy into technology from the start. She calls that concept “*Privacy by Design*.” While *Privacy by Design* began as a technology concept, it has evolved into a conceptual model for building an entire privacy program.

The fact is that *Privacy by Design* and accountability go together like innovation and high productivity. You can have one without the other, but it is hard.

A number of companies have been building programs where privacy is built into core business processes. One can find them in many industries and both business to business and business to consumer industries. Hewlett Packard has spent the last three years building a program called the “Accountability Model Tool” that integrates the technological concepts of *Privacy by Design* with the organizational commitment required for accountability. The accountability tool is now being implemented in the HP businesses that serve customers in 170 countries through 400,000 employees. This paper will describe accountability’s essential elements, the components of *Privacy by Design* and will use the HP “Accountability Model Tool” as an example of how leadership companies are building privacy in.

III The Essential Elements of Accountability

Accountability has a strong basis in privacy law and oversight. The Organization for Economic Cooperation and Development ("OECD") included accountability as principle eight in the Guidelines. Accountability is principle nine in the Asia Pacific Economic Cooperation forum ("APEC") Privacy Framework. It is principle one in the Model Code for the Protection of Personal Information (incorporated into Canadian law), and is a principle in the joint proposal drafted for consideration at the 31st International Conference of Data Protection and Privacy. However, none of those documents defined accountability as it applies to privacy.

The Centre for Information Policy Leadership at Hunton & Williams LLP, in a process facilitated by the Office of the Irish Data Protection Commissioner, brought together a group of experts to consider the essential elements of accountability in a project called the Galway Accountability Project. The Galway project held two experts discussions in Dublin, Ireland, the second sponsored by the OECD and the Business and Industry Advisory Council to the OECD. For the purpose of those discussions the group used the following working definition of accountability:

Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.

For an organization to have the capabilities to demonstrate its willingness to meet expectations based on law and organizational promises, and to have confidence in its ability to be answerable, the organization must have all aspects of privacy and information security under control. This is reflected in the essential elements of accountability:

1. An organization's 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. The means for remediation and external enforcement.

To be an accountable organization a company must have rules that are based on an external measuring stick such as data protection laws, industry self regulatory guidance, or guidance such as the OECD guidelines or APEC principles. Those policies must then be committed to by the organization at the highest level. The organization must have all the pieces in place to assure that the people who work at (employees) and for the organization (vendors) can be successful in implementing its policies and commitments. Furthermore, the organization must have internal measurement devices in place to assure the actions meet the words, and an external process to verify performance.

Privacy by Design is a process map for putting the essential elements of accountability into effect.

IV *Privacy by Design: 7 Foundational Principles*

Ontario Privacy Commissioner Ann Cavoukian has written that *Privacy by Design* is achieved by building fair information practice principles ("FIPs") into information technology, business practices, and physical design and infrastructures. This links with the accountability concepts in two ways. First the essential elements require that policies and practices must be based on external criteria. FIPs are the sum and substance of OECD and APEC privacy guidance, built into the European Union Data Protection Directive, and Canada's PIPEDA. They are examples of the external criteria referenced in the essential elements. Second, is the concept that the FIPs need to be built into all the processes from technology development to the physical structure of facilities. This too is required by the essential elements.

Dr. Cavoukian has also written that *Privacy by Design's* objectives may be accomplished through adoption of seven foundational principles:

1. Proactive not Reactive; Preventative not Reactive
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy.

Each of the foundation principles link to the essential elements of accountability.

1. ***Proactive not Reactive; Preventative not Reactive*** Proactive not reactive speaks to the accountability concept of having all the privacy policies as well as mechanisms in place so trained practitioners will see and resolve privacy issues before they turn into problems.
2. ***Privacy as the Default*** Accountability requires clear organizational rules with an explicit commitment to the policies that are the basis for those rules. Those rules will make clear that information should only be collected and used in a manner that is respectful of individual expectations and a safe information environment.
3. ***Privacy Embedded into Design*** Accountable business processes work best when privacy is embedded into design. This would be part of the mechanisms to implement policies.
4. ***Full Functionality – Positive Sum, Not Zero-Sum*** Organizations that understand privacy and bake privacy in have a better understanding of the risks to both the organization and to individuals. Organizations that build privacy in know how to create economic value while protecting individual privacy. The Centre

has been saying that clear privacy rules and methodologies create confident organizations that do not suffer from reticence risk.

5. **End-to-End Lifecycle Protection** End-to-end lifecycle protection informs the accountable organization that it must build privacy into every process from the assessment before data is collected to the oversight when data is retired.
6. **Visibility and Transparency** Principle six requires an organization to be open and honest with individuals. The accountable organization stands ready to demonstrate that it is open about what it does, stands behind its assertions, and is answerable when questions arise. The accountable organization provides the information necessary for individuals to participate consistent with the OECD individual participation principle. This is echoed in the *Privacy by Design* visibility and transparency principle.
7. **Respect for User Privacy** Lastly, the accountable organization must collect, use, store, share and retire information in a manner that is consistent with respect for the individual's privacy.

V Leadership Companies are Demonstrating *Privacy by Design*

In the course of the Centre's research we looked at leadership companies' information policy policies and practices. We saw information aggregators with excellent assurance review processes, software companies that build privacy protections into processes, and outsourcing companies with excellent checks and balances. "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment" by Paul Schwartz looked at the processes that six companies had for protecting privacy in an application that required data to cross borders. Professor Schwartz found all of the organizations to have very professional processes to assure data is used and protected appropriately.³

While there are many corporate examples of *Privacy by Design*, Hewlett Packard makes an interesting case study since they are in online retail, indirect retail, business-to-business, and services.

Privacy by Design – an HP Example

Globalization and new technologies are fundamentally changing how companies communicate and market to customers and prospects. It changes both the opportunities and the risks for individuals and organizations. Many of these technologies, including Web 2.0, user-generated content, and social media are straining traditional frameworks. And as the collection of data becomes more ubiquitous, data mining, analytics and behavioral targeting are growing more and more common and complex.

Laws and regulations often lag behind the practical realities of new technologies. This points to the fact that companies need to develop mechanisms that balance the tensions of using information robustly, yet ensure responsible decision making. Regulators and advocacy organizations are also looking to companies to demonstrate their capacity in upholding obligations and that their use and management of data is under control.

The *Privacy by Design* concepts, originally conceived by Commissioner Cavoukian, can be instantiated within a company in many ways. In an attempt to drive accountability throughout the enterprise, and ensure privacy considerations are taken into account at the earliest stages of a product's lifecycle, HP has developed a tool that guides employees.

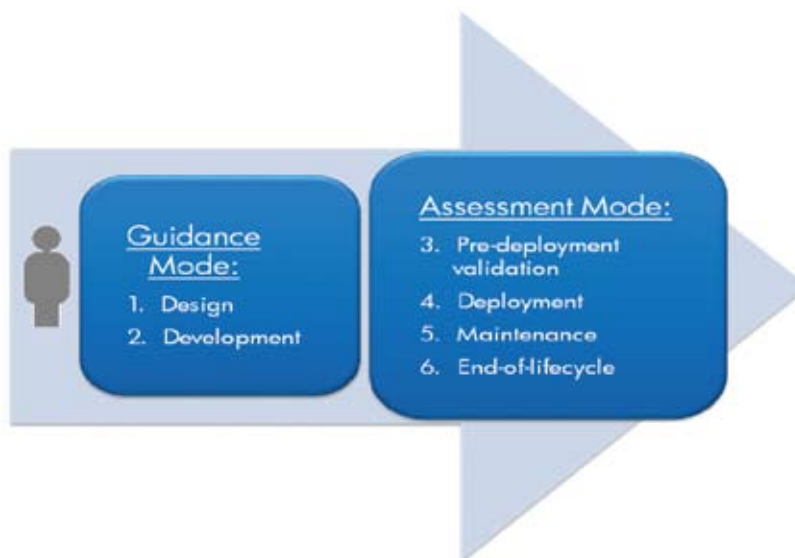
3 "Managing Global Information Privacy" is available on the OCED website (www.oecd.org) and The Privacy Projects, a NGO that sponsored the research

As this paper articulates, accountable practices can be broken down into three major categories: 1. Policies and Commitment, 2. Implementation Mechanisms, and 3. Assurance Practices. It is in the development of implementation mechanisms where *Privacy by Design* becomes critical. Employees of an organization must understand how to put policies, obligations, and values into effect. And to minimize business investment, reputation and compliance risks, employees need to consider privacy principles prior to design.



If a product or program is broken down into simple stages, it becomes clear when *Privacy by Design* guidance versus assessment needs to be applied. In the stages of Design and Development, the Privacy Office should provide proactive guidance so that privacy considerations can inform the planning stage. This is often missed and can result in a program being delayed or cancelled based on later privacy concerns.

Early guidance related to privacy becomes a tremendous value added to the organization. If caught early, privacy pitfalls can be avoided and good privacy practices embedded into the design of the program.



In the Pre-deployment, Deployment, Maintenance, and End-of-life stages, the Privacy Office needs to do more than just guide – they need to provide robust assessment mechanisms to ensure compliance with local laws, obligations, policies, and company values.

The assessment results should be documented and reviewed by the Privacy Office, consultation provided as necessary, and ultimately approved prior to deployment. After product or program launch, triggers should exist to ensure deployment was consistent with expectations and that end of life actions are taken when appropriate.

For many years, HP has been managing this *Privacy by Design* lifecycle through education, training, and encouraging employees to engage their privacy account manager at the early stages of design and development. As successful as this can be, it relies on employees thinking about privacy at the right time, knowing who to contact, and not feeling intimidated.

To solve these challenges and take *Privacy by Design* to a new level, the HP Privacy Office partnered with research scientists in HP Labs to develop a solution called the Accountability Model Tool. It combines the guidance in HP's existing Privacy Rulebook with a set of contextual, dynamically-generated questions. These two knowledge bases are connected through a sophisticated rules engine to help guide employees.

It allows employees and teams – working on simple marketing campaigns or complex product solutions – to see what privacy considerations need to be designed into their program. As described above, it works in both a guidance mode and in an assessment mode – depending on the lifecycle stage of the program.

Through company policy, employees who are collecting or using PII are required to assess their programs using this tool. It is easily accessible from the internal Privacy Intranet site. Using their digital badge they are authenticated and their basic contact and organizational information is automatically populated in the tool. All of their past projects are also accessible. This is important if an employee changes jobs or leaves the company so the Privacy Office knows which organization remains accountable for a program.

The tool begins by asking simple questions about the nature of their project. If it involves the collection or use of PII, they are presented with further contextual questions. As they answer each question, the next set of questions is dynamically generated based on how they answered prior questions. This is a critical component of success. The Privacy Office has found that each employee understands his or her area of expertise (e.g., e-mail marketing, product development, or employee relations), but when guidance and rules are not contextualized to their area of work, it becomes a daunting task for them to sift through hundreds of pages of rules or guidance and know how to apply them to their program. This tool is meant to narrow the context into exactly what they are doing and provide the associated guidance.

Profile questions

Project Information
Project Profile
Data sources/Data Flows
Transparency
Project Specifics
Harm Indicators

NOTE: This section presents questions that the tool uses to build up a basic profile of your project and to tailor follow-up questions in upcoming sections accordingly.

Does your project or activity (product, application, service, campaign, etc.) handle customer or employee information?

☒ Yes
☐ Not Sure
☐ Question is unclear

☐ No
☐ Question is unclear

Would you like the tool to provide privacy guidance or provide a privacy assessment of your project or activity? Please select your preferred mode(s).

☐ Privacy Guidance
☒ Privacy Assessment
☐ Question is unclear

Which information categories does your project or activity handle? (check all that apply)

☐ Customer information
☐ Other
☐ Employee information

Questionnaire is dynamically "built" so it is relevant & the user doesn't have to answer unnecessary questions.

By asking employees contextual questions – and linking their answers immediately against the rules database – the tool not only guides, but educates the employee on good privacy practices. For each question, terms are defined by using text rollovers and help is provided that links the employee directly into the HP Privacy Rulebook. They can also check a box that says "Question is Unclear." This allows the Privacy Office to track trends and improve the delivery of questions if patterns evolve.

The tool takes the employee through a series of questions related to the profile and nature of the project, data sources and flows, transparency, compliance, and indicators of any issues that might arise or surprise the data subject. Once the employee has completed the questions, a report is generated that shows an overall rating, as well as areas of compliance and non-compliance.

Assessment Report

Project Information

This section provides details of the project.

Leading Organization: PSG Asia Pacific & Japan
Leading Business Unit: Emerging Markets (PSG)
Leading Business Group: Personal Systems Group-PSG
Project/Campaign Region: Asia Pacific
Project Lead: Allan Paull
Lead Email: allan.paull@hp.com
Owner Name: Allan Paull
Owner Title: null
Owner's Phone: +61 411 232 249
Owner's E-mail: allan.paull@hp.com
Edited by: allan.paull@hp.com

Summary Of Findings



eMail marketing campaign test has been found to be **compliant** by the HP Privacy Account. Please contact the Privacy Office if you would like to discuss any related issues.

Summary of findings

Risk Indicators

Risk indicators graph

This graph shows the number of green, yellow and red flags triggered for each risk indicator.

For areas of non-compliance, reasons are provided, including links to further information and checklists that can be used to achieve compliance.

Detailed information per risk indicator



A. Transborder data flow

The following low risks have been identified:



B. HP compliance/Non-compliance

The following low risks have been identified:



C. Other

The following moderate risks have been identified:



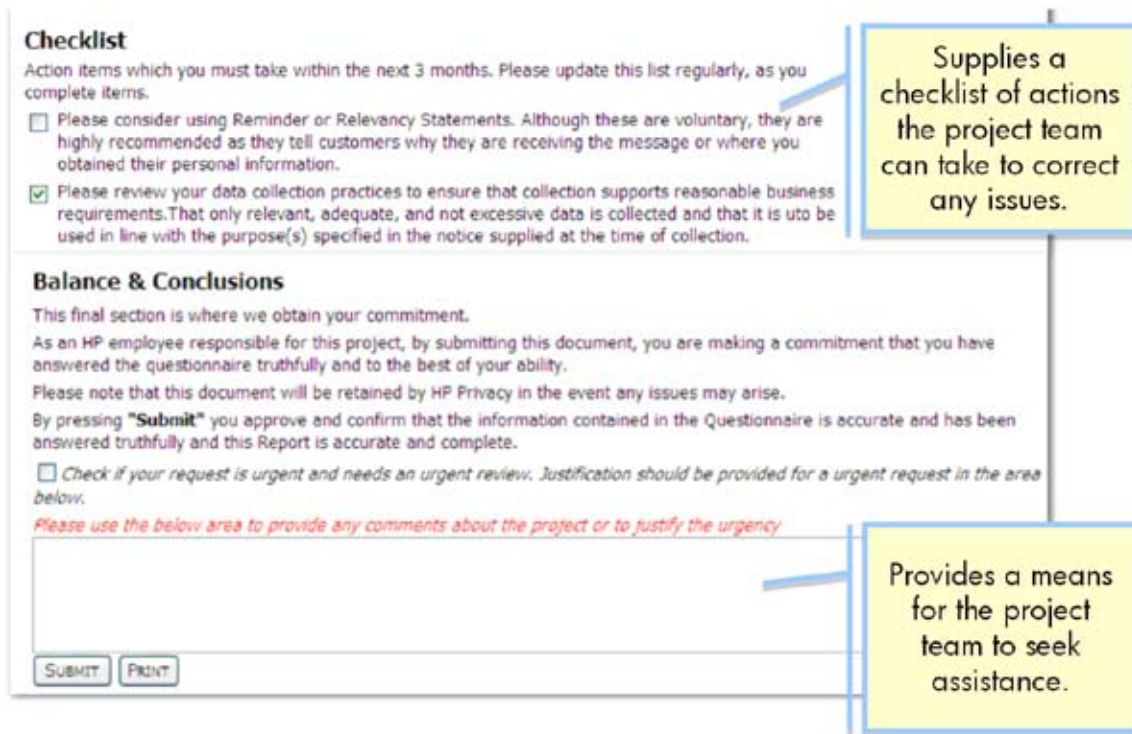
Relevancy statements are highly recommended, but not required. Relevancy Statement: Tell customers why they are receiving the message or where you obtained their personal information. Can appear in the introduction, body, or footer of the message; recommended placement is in the introduction.

- One-to-One Sales: In response to your request
- One-to-One Transactional: You are receiving this message because you reported an issue to our call center
- One-to-Many Marketing: You are receiving this message because it matches your current subscription profile
- One-to-Many Transactional: In response to your request. You are receiving this message as part of your service agreement with HP
- Joint Marketing: You are receiving this advertisement from HP and [insert partner name] because HP and [insert partner name] offer complementary solutions that match the interests

[View details](#)

Details of compliance & non-compliance

Once the employee has made the appropriate modifications, he or she can submit their report to the HP Privacy Office where it will be reviewed and archived.



Checklist
Action items which you must take within the next 3 months. Please update this list regularly, as you complete items.

- ☐ Please consider using Reminder or Relevancy Statements. Although these are voluntary, they are highly recommended as they tell customers why they are receiving the message or where you obtained their personal information.
- ☒ Please review your data collection practices to ensure that collection supports reasonable business requirements. That only relevant, adequate, and not excessive data is collected and that it is used in line with the purpose(s) specified in the notice supplied at the time of collection.

Balance & Conclusions
This final section is where we obtain your commitment.
As an HP employee responsible for this project, by submitting this document, you are making a commitment that you have answered the questionnaire truthfully and to the best of your ability.
Please note that this document will be retained by HP Privacy in the event any issues may arise.
By pressing "Submit" you approve and confirm that the information contained in the Questionnaire is accurate and has been answered truthfully and this Report is accurate and complete.

☐ Check if your request is urgent and needs an urgent review. Justification should be provided for a urgent request in the area below.

Please use the below area to provide any comments about the project or to justify the urgency

Callouts:

- Supplies a checklist of actions the project team can take to correct any issues.
- Provides a means for the project team to seek assistance.

They are attesting to the truth and accuracy of their statements and will be held accountable. For any areas of concern, the Privacy Office must approve the program prior to deployment.

Once approved, the program information is warehoused in the database. It is maintained for future use as well as a trigger for ongoing assurance monitoring. This database of projects provides a real-time dashboard for the Privacy Office, allows improved ongoing communications and ensures that if laws or regulations in a country change that programs can be modified as appropriate.

This is a new program for HP and has just been deployed. It is a valuable tool along with ongoing efforts in training, implementation standards, compliance management, and audit. It achieves Commissioner Cavoukian's concepts for *Privacy by Design* in a manner that is systematic, predictable and repeatable – and ultimately will drive a richer culture of privacy within the enterprise. It also will enable HP to better demonstrate commitment and capacity in upholding privacy promises and obligations.

VI Conclusion

In this paper, we have seen an excellent example of how enhanced privacy accountability and assurance can be achieved within an organization by applying *Privacy by Design* principles, in a thoroughgoing manner.

So imperative today are the goals of enhanced accountability and assurance, so universal are the PbD principles, and so diverse are the contexts within which these principles may be applied, that the future of privacy in the 21st century information age may be limited only by our collective imagination and will.

There are virtually infinite ways by which organizations can creatively “build privacy in” to their operations and products, to earn the confidence and trust of customers, business partners and oversight bodies alike, and to be leaders in the global marketplace.

We need to acknowledge and celebrate these innovations and successes, and steadily build upon them.

About the Authors

Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

Martin E. Abrams, Senior Policy Advisor and Executive Director, Centre for Information Policy Leadership, Hunton & Williams LLP

Martin Abrams is Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP, a global privacy and information security think tank, and an advisor to the Business Forum for Consumer Privacy. Mr. Abrams brings more than 30 years' experience as a policy innovator to the Centre, where he pursues practical solutions to privacy and security problems. He is a leading theorist on global transfers of data based on accountability, and has led the movement in the U.S. to adopt harms-based approaches to privacy. He was a leader in developing layered privacy notices, and is currently working to bridge cultural differences in privacy. Mr. Abrams has led privacy programs on five continents, and is part of the APEC Data Privacy Subgroup.

Scott Taylor, Chief Privacy Officer, Hewlett-Packard Company

As head of HP's privacy and data protection efforts worldwide, Scott Taylor is responsible for global privacy strategy, policy, governance, and operations. In this role, he is a member of HP's Ethics & Compliance Council, Global Citizenship Committee, and chairs HP's Privacy & Data Protection Governance Board. Taylor and his team work with HP business groups, regions and corporate functions to assure the implementation of HP's privacy policies and programs and integrate privacy into product and services development across the company. He serves as HP's global representative with external policy-makers, media, NGOs and customers in the area of privacy and data protection. Taylor serves on the Board of Directors for The Business Forum for Consumer Privacy, as the Chairman of the Executive Council at The Center for Information Policy Leadership, and on the Board of Directors for the Council of Better Business Bureaus. Taylor has been with HP for 22 years. Previously he led HP's global Internet program, part of the Global Operations Organization. In that role, he and his team handled Internet strategy, customer experience, e-business policies, standards, worldwide site management, and operations. Taylor led the team that launched HP's Internet presence in 1994 and managed it for 12 years. Prior to that, Taylor was responsible for HP's direct marketing function, part of the Corporate Marketing & International Services Organization.



Information and Privacy Commissioner of Ontario, Canada

2 Bloor Street East
Suite 1400

Toronto, Ontario M4W 1A8
Canada

Telephone: 416-326-3333

Fax: 416-325-9195

Website: www.ipc.on.ca

Privacy by Design: www.privacybydesign.ca

The Centre for Information Policy Leadership

at Hutton & Williams LLP

1900 K Street, NW
Washington, DC 20006
USA

Telephone: 202-955-1500

Fax: 202-778-2201

Website: www.informationpolicycentre.com

Hewlett-Packard (Canada) Co.

5150 Spectrum Way
Mailstop 6H72

Mississauga, Ontario L4W 5G1
Canada

Telephone: 905-206-4725

Fax: 905-206-4739

Website: www.hp.ca

The information contained herein is subject to change without notice. HP, CIPL - Hutton & Williams, LLP, and IPC shall not be liable for technical or editorial errors or omissions contained herein.



World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 10, Number 10

October 2010

Accountability: Part Of The International Public Dialogue About Privacy Governance

By Paula J. Bruening, Centre for Information Policy Leadership at Hunton & Williams LLP, Washington.

Dramatic advances in the speed, volume and complexity of data flows challenge existing models of data protection. Powerful analytics yield deeply insightful, real-time inferences about computer users that enhance the online experience and enable companies to offer products and services to the right individual at the right time. Behavioral targeting uses a complex network of vendors to track and analyze an individual's online activity to serve tailored, more effective advertising. Organizations collect and derive data about individuals from myriad sources and often employ service vendors located halfway around the world to carry out internal business processes and provide around-the-clock customer service. Using technologies ranging from surveillance cameras to radio frequency identification, they gather and store data cheaply, often in the cloud, where servers may be located on another continent. And given the rapid pace of development, an organization's impulse to retain that information for future, as yet unanticipated, uses is understandable and often makes good business sense.

The growing power of data holds the promise of economic benefit for businesses and consumers. But to realize that potential, consumers must be confident that their information is used responsibly, and that their privacy is protected. Over the last 18 months, policy-

makers around the world have undertaken efforts to examine and update data governance in a way that would better serve this rapidly changing data environment, providing the best possible privacy protection while encouraging innovation and flexible data use. While policymakers continue to cite traditional principles of fair information practice as relevant and the foundation of good privacy and data protection, they recognize the challenges new technologies and business models pose to the application of those principles.

Data protection that relies primarily on notice and choice has come under particular scrutiny. In a notice-and-choice model, consumers receive information about how an organization will collect, use, and share data about them. On the basis of this notification, consumers choose whether to allow its use. Such a model is seriously challenged by an environment in which organizations can analyze and process information instantaneously at the collection point, and where data collection has become so ubiquitous that individuals could easily be overwhelmed by the privacy notices they receive each day as they shop online, use a mobile communications device, engage in social networking, or visit a building that uses surveillance cameras or sensor technology. In many cases, it is impossible to provide notice, and even when it is, notices are lengthy and complex. Given that data use is necessary for so many activities, both online and offline, choice itself

may be possible and provide real guidance for organizations about how to use information only in limited circumstances.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed.

Faced with these challenges, policymakers are asking a number of questions. How best to protect the privacy of individuals, even when choice is not meaningful or in some instances not possible? How to encourage the innovation in data use that encourages economic growth and still safeguard individuals' interests in the protection and responsible use of their data? For possible answers, policymakers have turned their attention to the fair information practice principle of *accountability*.

Accountability as a principle of data protection is not new. It was first articulated in 1980 as a principle of fair information practices in the Organization for Economic Cooperation and Development's (OECD) privacy guidelines.¹ The accountability principle places responsibility on organizations as data controllers "for complying with measures that give effect" to all eight of the OECD guidelines' principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly articulated in the EU Data Protection Directive (95/46/EC), numerous provisions require that organizations 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. It is the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),² which requires that Canadian organizations implement the full complement of PIPEDA principles, whether the data are processed by the organization or outside vendors, or within or outside Canada. In the United States, accountability underpins the security requirements of the Gramm-Leach-Bliley Act, which requires that organizations secure their data holdings against theft, loss or unauthorized access, but leaves to their discretion the most effective way to do so.

Accountability Project

Until now, the principle of accountability has often gone undefined, and it has been unclear what conditions organizations must create to establish and demonstrate their accountability. As it has begun to play an increasingly visible role in privacy governance, an international group of experts — including business leaders, data protection authorities, advocates, and government representatives — have convened the Accountability Project. Organized by the Centre for Information Policy Leadership, the Accountability Project seeks to define the contours of accountability, to articulate how it is demonstrated and measured, and to establish why individuals should trust it to protect their data. Their work began as

an inquiry into the essential elements of accountability in early 2009, and will continue into 2011 to more concretely define the fundamentals that characterize the accountable organization.

According to the Project, accountability is designed to provide robust protections for data while avoiding aspects of current data protection that may be of limited effect or that may burden organizations without yielding commensurate privacy benefits. Accountability allows the organization greater flexibility to adapt its data practices to serve emerging business models and technologies and to meet consumer demand. In exchange, it requires that the organization commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a way that protects information and the individuals to which it pertains.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed. An accountability-based approach to data governance focuses on setting privacy-protection goals for organizations based on criteria established in current public policy and allowing organizations discretion in determining how those goals are met. Accountable organizations will adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the demands of their customers.

The essential elements of accountability are:

1) Organization commitment to accountability and adoption of internal policies consistent with external criteria

An organization demonstrates its willingness and ability to be responsible and answerable for its data practices. Its practices are based on policies consistent with appropriate external criteria — applicable law, generally accepted principles, and/or industry best practices. Practices are designed to provide the individual with effective privacy protection.

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

The accountable organization deploys and monitors mechanisms and internal programs that ensure its privacy policies are carried out. Mechanisms may include tools to facilitate decision making about data use and protection, training about how to use those tools and processes to ensure employee compliance.

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

The organization monitors and assesses whether its internal policies manage, protect and secure data effectively. Risk analysis appropriate to the organization and the industry in which it functions is key to successful monitoring and risk management. The accountable organization engages, as appropriate, an independent entity to verify and demonstrate that it meets the requirements of accountability.

4) Transparency and mechanisms for individual participation

Accountability requires transparency. The accountable organization effectively communicates to indi-

viduals critical information about its data procedures and protections in a posted privacy notice. When appropriate, the information in the privacy notice can provide the basis for the consumer's consent or choice. Individuals should be able to see the data or types of data that the organization 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. In some cases, however, public policy reasons will limit that disclosure.

5) Means for remediation and external enforcement

The accountable organization establishes a means to address harm to individuals caused by the failure of internal policies and practices. When harm occurs due to a failure of an organization's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. The organization should identify an individual to serve as the first point of contact for resolution of disputes and establish a process to review and address complaints.³

Developers envision the ability of an accountability approach to improve data protection in several ways. Ideally, accountability will:

- help organizations 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 respond quickly to new business models and emerging technologies;
- enable organizations to better deploy scarce resources allocated to privacy protection. Resources devoted to administrative requirements such as notification of data authorities of minor changes in processing can be redirected to more effective protection measures that most effectively safeguard data;
- heighten the confidence of individuals that their data will be protected wherever it is stored or processed; and
- bridge data protection regimes across jurisdictions, but allow countries to pursue common data protection objectives through very different but equally reliable means.

Accountability does not preclude application of principles of fair information practices. It does relieve the individual of much of the burden of policing the marketplace for organizations 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. In an accountability model, when the consumer can provide meaningful consent, the organization is required to act based on that consent. But even when the consumer cannot, accountability demands responsible, disciplined data storage, use and protection.

Factor in International Discussions

Accountability has begun to figure prominently in ongoing discussions about effective data protection.

Accountability has come under close review in the European Union. The Article 29 Working Party launched a consultation on the EU data protection legal framework and determined that the level of data protection in the European Union could benefit from better application of existing data protection principles in practice. In an article released in December 2009 entitled "The Future of Privacy,"⁴ the Article 29 Data Protection Working Party and the Working Party on Policy and Justice noted that, while traditional principles of data protection remain valid, new technologies and the global flow of data present new challenges to data protection. They characterized the new challenges as an opportunity to, among other things, introduce additional principles, including accountability. It also noted the need to strengthen the effectiveness of the current system through modernization, citing particularly the need to reduce bureaucratic burdens.

In July 2010, the Article 29 Working Party released an opinion focusing specifically on accountability⁵ (*see analysis in this issue*). According to the opinion, a principle of accountability "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the [Data Protection] Directive and demonstrate this on request." The Working Party's objective is to "encourage data protection in practice" by requiring data controllers to engage in risk assessment and adopt measures such as:

- data loss/breach detection/prevention policies and procedures;
- "Privacy by Design" in the development and implementation of new technologies;
- binding policies and procedures that measure compliance; and
- response plans that draw on the organization's experience, mitigate harm and discourage future breaches.

At the Asia-Pacific Economic Cooperation, the Privacy Framework⁶ depends upon accountability to facilitate cross-border data flows. In language similar to that in the OECD Guidelines, the APEC Framework provides that "[a] personal information controller should be accountable for complying with measures that give effect to the Principles stated above."

The Framework commentary specifically discusses accountability in the context of information transfers between different types of organizations, in different locations. It states that controllers should be accountable for ensuring that the recipient of the information will protect it in accordance with the Framework principles. Under the APEC Framework, controllers are accountable for protection of the data even after it is transferred for processing or storage. The requirement assumes that the controller will conduct due diligence to ensure that the recipient is able and committed to fulfilling the obligations to manage and protect the data appropriately.

Finally, the proposed "International Standards on the Protection of Personal Data and Privacy" that are the subject of the Madrid Resolution⁷ also incorporate the

principle of accountability. The principle recognizes both the obligation to observe all of the principles and obligations in the proposed standard, and takes the additional step to require that organizations implement mechanisms and be able to demonstrate their compliance.

Summary

Accountability has become part of the international public dialogue about privacy governance. But to be an effective, credible solution to the privacy issues raised by 21st century data use, it will be necessary to establish the fundamentals that would make an accountability model work in practice.

The Accountability Project is engaged in additional collaborative work to explore the practical questions related to implementing and administering an accountability approach. What must an organization demonstrate to be deemed accountable? How is accountability measured? What triggers an accountability review? How will remediation work in an accountability approach?

Resolution of these and other questions by international policymakers, business, experts and advocates will be critical to accountability's successful adoption as an innovative, effective approach to privacy and data protection.

NOTES

¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

² <http://laws.justice.gc.ca/en/P-8.6/>

³ For a more comprehensive discussion of accountability, see "Data Protection Accountability: A Document for Discussion," October 2009, <http://www.ftc.gov/os/comments/privacyproundtable/544506-00059.pdf>.

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." 02356/09EN/ WP 168, December 1, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

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

⁶ The APEC Privacy Framework, published 2005, <http://op.bna.com/pl.nsf/r?Open=byul-89js2b>

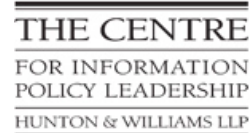
⁷ "Internacional Standards on the Protection of Personal Data and Privacy: The Madrid Resolution," released October 2009, <http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf>.

Paula J. Bruening is Deputy Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP in Washington. She may be contacted at pbruening@hunton.com.

Privacy by Design: Essential for Organizational Accountability and Strong Business Practices



November 2009



Acknowledgements

The authors wish to acknowledge Fred Carter, Senior Policy and Technology Advisor, Policy Department at the Information and Privacy Commissioner's Office, Ontario, Canada for his input on this paper, as well as Susan Smith, Americas Privacy Officer, Hewlett-Packard Company and staff at The Centre for Information and Policy Leadership at Hunton & Williams LLP.

Table of Contents

Foreword	1
I Introduction.....	3
II Convergence of Accountability and <i>Privacy by Design</i>	4
III The Essential Elements of Accountability.....	5
IV <i>Privacy by Design</i> : 7 Foundational Principles.....	6
V Leadership Companies are Demonstrating <i>Privacy by Design</i>	8
<i>Privacy by Design</i> – an HP Example	8
VI Conclusion	14

Foreword

The proposition that “privacy is good for business” is one that is enshrined in all Fair Information Practices (FIPs) around the world and, through them, in the many laws and organizational practices upon which they are based. By setting out universal principles for handling personal data, FIPs seek to ensure the privacy of individuals *and* to promote the free flow of personal data and, through them the growth of commerce.

The enduring confidence of individuals, business partners and regulators in organizations’ data-handling practices is a function of their ability to express the FIPs’ core requirements. These are: to limit collection, use and disclosure of personal data; to involve individuals in the data lifecycle, and to apply appropriate safeguards in a thoroughgoing manner. These requirements, in turn, are premised upon organizational openness and accountability. The ultimate results – which are highly desirable – include enhanced trust, improved efficiencies, greater innovation, and a heightened competitive advantage. Privacy *is* good for business.

But the early FIPs drafters and adopters had in mind large mainframe computers and centralized electronic databases. They could never have imagined how leapfrogging revolutions in sensors, bandwidth, storage, and processing power would converge into our current hyper-connected “Web 2.0” networked world of ubiquitous data availability.

It has become trite to observe that data is the lifeblood of the new economy, but who today can truly grasp how large the arteries are becoming, how they are multiplying, where they may lead, and to what end? Everywhere we see near-exponential growth of data creation, transmission, use and storage, by an ever-expanding universe of actors, somewhere out there in the opaque “cloud.” Most of this data is personally-identifiable. And most of it is now controlled by someone other than the individual himself or herself. Thanks to new information flows, today we enjoy unprecedented and nearly unimaginable new services and benefits, but these have been accompanied by unprecedented and once unimaginable privacy threats and harms. Some say that privacy is effectively dead or dying in the information age. We say that it is not, but it *is* rapidly changing shape.

The need for organizational accountability remains constant – indeed, it has become more urgent today than ever before. What is changing are the *means* by which accountability may be demonstrated, whether to individuals, regulators or to business partners. Beyond policy statements, what is needed now are more innovative and more robust methods for assuring that personal data is, in fact, being managed responsibly.

There are many paths to enhanced accountability and assurance, typically involving a mix of technology, policies and practices, and of law and regulation. More than ever before, a comprehensive and proactive *Privacy by Design* approach to information management is called for – one which assures an end-to-end chain of custody and responsibility right from the very start.

Scott Taylor
Chief Privacy Officer
Hewlett-Packard
Company

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Martin E. Abrams
Senior Policy Advisor and
Executive Director
Centre for Information
Policy Leadership,
Hunton & Williams LLP

I Introduction

Professor Paul A. Schwartz recently wrote:

“Companies are now putting internal policies in place, centered on forward looking rules of information management and training of personnel. Such policies are, at the very least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection.”¹

An accountability-based regulatory structure is one where organizations are charged with societal objectives, such as using information in a manner that maintains individual autonomy and protecting the individual from social, financial and physical harms that might come from the mismanagement of information, while leaving the actual mechanisms for achieving those objectives to the organization. One of the best conceptual models for building in the types of controls suggested by Professor Schwartz is *Privacy by Design*. The best in class companies in Schwartz’s study, “Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment,” are using *Privacy by Design* concepts to build business process that use personal information robustly with clear privacy-protective controls built into every facet of the business process. In other words, *Privacy by Design* and accountability go together in much the same way that innovation and productivity go together.

Accountability is the governance model that is based on organizations taking responsibility for protecting privacy and information security appropriately and protecting individuals from the negative outcomes associated with privacy-protection failures. Accountability was first framed as a privacy principle in the OECD Privacy Guidelines.

The Centre for Information Policy Leadership at Hunton & Williams LLP has recently acted as secretariat for the Galway project that defined the essential elements of accountability.

The conceptual model, *Privacy by Design*, was developed by Ontario Privacy Commissioner Ann Cavoukian in the 1990s to address the development of technologies, but she has since expanded it to include business processes.²

Hewlett Packard is in the midst of implementing an accountability tool built on both accountability principles and the key concepts of *Privacy by Design*. HP’s accountability tool is an example of the trend described by Professor Schwartz.

This paper discusses the essential elements of accountability, *Privacy by Design* principles, and provides an example of a control process that uses the principles to implement the essential elements.

1 “Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment,” Paul A. Schwartz, a working paper by The Privacy Projects, October 2009.

2 “Privacy by Design,” Ann Cavoukian, Ph.D., January 2009.

II *Convergence of Accountability and Privacy by Design*

Accountability as both a basic privacy implementation and enforcement principle dates to the approval of the OECD Privacy Framework in 1980. But it is only today that the privacy community is beginning to understand what is meant by accountability-based privacy governance, and how it impacts the structuring of a privacy program. The growth of Binding Corporate Rules in the European Union, Cross-Border Privacy Rules in APEC, Safe Guard concepts in the United States, and data transfers compliant with the Personal Information and Electronic Documents Act (PIPEDA) in Canada has made clear direction on accountability crucial. The Galway project published a paper called “Data Protection Accountability: The Essential Elements,” in October 2009 that enumerated five essential elements for accountability. The paper was developed with a distinguished group of privacy experts from privacy enforcement agencies, government, academia, civil society and business, and facilitated by the Office of the Irish Data Protection Commissioner, and chaired by the Centre. The essential elements make it clear that accountability comes from privacy protections based on commitment to a program where privacy is built into all business processes.

Over a decade ago Ontario Privacy Commissioner Ann Cavoukian began discussing the virtues of building privacy into technology from the start. She calls that concept “*Privacy by Design*.” While *Privacy by Design* began as a technology concept, it has evolved into a conceptual model for building an entire privacy program.

The fact is that *Privacy by Design* and accountability go together like innovation and high productivity. You can have one without the other, but it is hard.

A number of companies have been building programs where privacy is built into core business processes. One can find them in many industries and both business to business and business to consumer industries. Hewlett Packard has spent the last three years building a program called the “Accountability Model Tool” that integrates the technological concepts of *Privacy by Design* with the organizational commitment required for accountability. The accountability tool is now being implemented in the HP businesses that serve customers in 170 countries through 400,000 employees. This paper will describe accountability’s essential elements, the components of *Privacy by Design* and will use the HP “Accountability Model Tool” as an example of how leadership companies are building privacy in.

III The Essential Elements of Accountability

Accountability has a strong basis in privacy law and oversight. The Organization for Economic Cooperation and Development ("OECD") included accountability as principle eight in the Guidelines. Accountability is principle nine in the Asia Pacific Economic Cooperation forum ("APEC") Privacy Framework. It is principle one in the Model Code for the Protection of Personal Information (incorporated into Canadian law), and is a principle in the joint proposal drafted for consideration at the 31st International Conference of Data Protection and Privacy. However, none of those documents defined accountability as it applies to privacy.

The Centre for Information Policy Leadership at Hunton & Williams LLP, in a process facilitated by the Office of the Irish Data Protection Commissioner, brought together a group of experts to consider the essential elements of accountability in a project called the Galway Accountability Project. The Galway project held two experts discussions in Dublin, Ireland, the second sponsored by the OECD and the Business and Industry Advisory Council to the OECD. For the purpose of those discussions the group used the following working definition of accountability:

Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.

For an organization to have the capabilities to demonstrate its willingness to meet expectations based on law and organizational promises, and to have confidence in its ability to be answerable, the organization must have all aspects of privacy and information security under control. This is reflected in the essential elements of accountability:

1. An organization's 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. The means for remediation and external enforcement.

To be an accountable organization a company must have rules that are based on an external measuring stick such as data protection laws, industry self regulatory guidance, or guidance such as the OECD guidelines or APEC principles. Those policies must then be committed to by the organization at the highest level. The organization must have all the pieces in place to assure that the people who work at (employees) and for the organization (vendors) can be successful in implementing its policies and commitments. Furthermore, the organization must have internal measurement devices in place to assure the actions meet the words, and an external process to verify performance.

Privacy by Design is a process map for putting the essential elements of accountability into effect.

IV *Privacy by Design: 7 Foundational Principles*

Ontario Privacy Commissioner Ann Cavoukian has written that *Privacy by Design* is achieved by building fair information practice principles ("FIPs") into information technology, business practices, and physical design and infrastructures. This links with the accountability concepts in two ways. First the essential elements require that policies and practices must be based on external criteria. FIPs are the sum and substance of OECD and APEC privacy guidance, built into the European Union Data Protection Directive, and Canada's PIPEDA. They are examples of the external criteria referenced in the essential elements. Second, is the concept that the FIPs need to be built into all the processes from technology development to the physical structure of facilities. This too is required by the essential elements.

Dr. Cavoukian has also written that *Privacy by Design's* objectives may be accomplished through adoption of seven foundational principles:

1. Proactive not Reactive; Preventative not Reactive
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy.

Each of the foundation principles link to the essential elements of accountability.

1. ***Proactive not Reactive; Preventative not Reactive*** Proactive not reactive speaks to the accountability concept of having all the privacy policies as well as mechanisms in place so trained practitioners will see and resolve privacy issues before they turn into problems.
2. ***Privacy as the Default*** Accountability requires clear organizational rules with an explicit commitment to the policies that are the basis for those rules. Those rules will make clear that information should only be collected and used in a manner that is respectful of individual expectations and a safe information environment.
3. ***Privacy Embedded into Design*** Accountable business processes work best when privacy is embedded into design. This would be part of the mechanisms to implement policies.
4. ***Full Functionality – Positive Sum, Not Zero-Sum*** Organizations that understand privacy and bake privacy in have a better understanding of the risks to both the organization and to individuals. Organizations that build privacy in know how to create economic value while protecting individual privacy. The Centre

has been saying that clear privacy rules and methodologies create confident organizations that do not suffer from reticence risk.

5. **End-to-End Lifecycle Protection** End-to-end lifecycle protection informs the accountable organization that it must build privacy into every process from the assessment before data is collected to the oversight when data is retired.
6. **Visibility and Transparency** Principle six requires an organization to be open and honest with individuals. The accountable organization stands ready to demonstrate that it is open about what it does, stands behind its assertions, and is answerable when questions arise. The accountable organization provides the information necessary for individuals to participate consistent with the OECD individual participation principle. This is echoed in the *Privacy by Design* visibility and transparency principle.
7. **Respect for User Privacy** Lastly, the accountable organization must collect, use, store, share and retire information in a manner that is consistent with respect for the individual's privacy.

V Leadership Companies are Demonstrating *Privacy by Design*

In the course of the Centre's research we looked at leadership companies' information policy policies and practices. We saw information aggregators with excellent assurance review processes, software companies that build privacy protections into processes, and outsourcing companies with excellent checks and balances. "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment" by Paul Schwartz looked at the processes that six companies had for protecting privacy in an application that required data to cross borders. Professor Schwartz found all of the organizations to have very professional processes to assure data is used and protected appropriately.³

While there are many corporate examples of *Privacy by Design*, Hewlett Packard makes an interesting case study since they are in online retail, indirect retail, business-to-business, and services.

Privacy by Design – an HP Example

Globalization and new technologies are fundamentally changing how companies communicate and market to customers and prospects. It changes both the opportunities and the risks for individuals and organizations. Many of these technologies, including Web 2.0, user-generated content, and social media are straining traditional frameworks. And as the collection of data becomes more ubiquitous, data mining, analytics and behavioral targeting are growing more and more common and complex.

Laws and regulations often lag behind the practical realities of new technologies. This points to the fact that companies need to develop mechanisms that balance the tensions of using information robustly, yet ensure responsible decision making. Regulators and advocacy organizations are also looking to companies to demonstrate their capacity in upholding obligations and that their use and management of data is under control.

The *Privacy by Design* concepts, originally conceived by Commissioner Cavoukian, can be instantiated within a company in many ways. In an attempt to drive accountability throughout the enterprise, and ensure privacy considerations are taken into account at the earliest stages of a product's lifecycle, HP has developed a tool that guides employees.

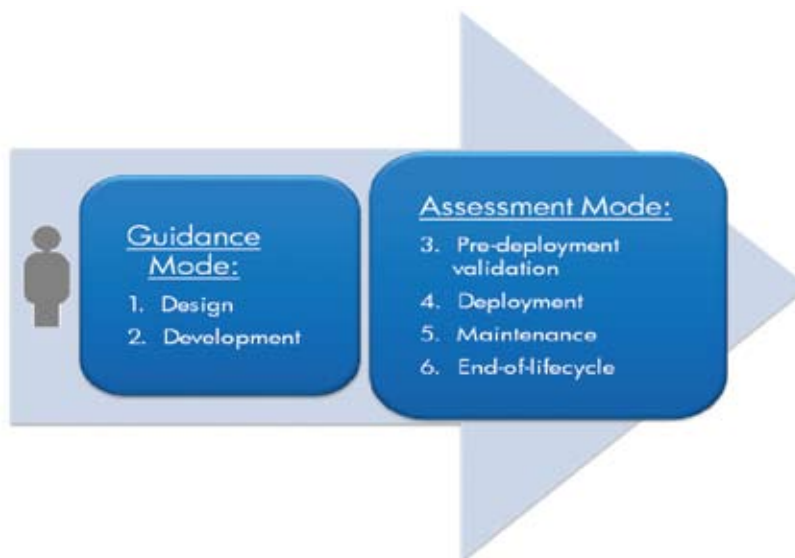
³ "Managing Global Information Privacy" is available on the OCED website (www.oecd.org) and The Privacy Projects, a NGO that sponsored the research

As this paper articulates, accountable practices can be broken down into three major categories: 1. Policies and Commitment, 2. Implementation Mechanisms, and 3. Assurance Practices. It is in the development of implementation mechanisms where *Privacy by Design* becomes critical. Employees of an organization must understand how to put policies, obligations, and values into effect. And to minimize business investment, reputation and compliance risks, employees need to consider privacy principles prior to design.



If a product or program is broken down into simple stages, it becomes clear when *Privacy by Design* guidance versus assessment needs to be applied. In the stages of Design and Development, the Privacy Office should provide proactive guidance so that privacy considerations can inform the planning stage. This is often missed and can result in a program being delayed or cancelled based on later privacy concerns.

Early guidance related to privacy becomes a tremendous value added to the organization. If caught early, privacy pitfalls can be avoided and good privacy practices embedded into the design of the program.



In the Pre-deployment, Deployment, Maintenance, and End-of-life stages, the Privacy Office needs to do more than just guide – they need to provide robust assessment mechanisms to ensure compliance with local laws, obligations, policies, and company values.

The assessment results should be documented and reviewed by the Privacy Office, consultation provided as necessary, and ultimately approved prior to deployment. After product or program launch, triggers should exist to ensure deployment was consistent with expectations and that end of life actions are taken when appropriate.

For many years, HP has been managing this *Privacy by Design* lifecycle through education, training, and encouraging employees to engage their privacy account manager at the early stages of design and development. As successful as this can be, it relies on employees thinking about privacy at the right time, knowing who to contact, and not feeling intimidated.

To solve these challenges and take *Privacy by Design* to a new level, the HP Privacy Office partnered with research scientists in HP Labs to develop a solution called the Accountability Model Tool. It combines the guidance in HP's existing Privacy Rulebook with a set of contextual, dynamically-generated questions. These two knowledge bases are connected through a sophisticated rules engine to help guide employees.

It allows employees and teams – working on simple marketing campaigns or complex product solutions – to see what privacy considerations need to be designed into their program. As described above, it works in both a guidance mode and in an assessment mode – depending on the lifecycle stage of the program.

Through company policy, employees who are collecting or using PII are required to assess their programs using this tool. It is easily accessible from the internal Privacy Intranet site. Using their digital badge they are authenticated and their basic contact and organizational information is automatically populated in the tool. All of their past projects are also accessible. This is important if an employee changes jobs or leaves the company so the Privacy Office knows which organization remains accountable for a program.

The tool begins by asking simple questions about the nature of their project. If it involves the collection or use of PII, they are presented with further contextual questions. As they answer each question, the next set of questions is dynamically generated based on how they answered prior questions. This is a critical component of success. The Privacy Office has found that each employee understands his or her area of expertise (e.g., e-mail marketing, product development, or employee relations), but when guidance and rules are not contextualized to their area of work, it becomes a daunting task for them to sift through hundreds of pages of rules or guidance and know how to apply them to their program. This tool is meant to narrow the context into exactly what they are doing and provide the associated guidance.

Profile questions

Project Information
Project Profile
Data sources/Data Flows
Transparency
Project Specifics
Harm Indicators

NOTE: This section presents questions that the tool uses to build up a basic profile of your project and to tailor follow-up questions in upcoming sections accordingly.

Does your project or activity (product, application, service, campaign, etc.) handle customer or employee information?

☒ Yes
☐ Not Sure
☐ Question is unclear
☐ No

Would you like the tool to provide privacy guidance or provide a privacy assessment of your project or activity? Please select your preferred mode(s).

☐ Privacy Guidance
☒ Privacy Assessment
☐ Question is unclear

Which information categories does your project or activity handle? (check all that apply)

☐ Customer information
☐ Other
☐ Employee information

Questionnaire is dynamically "built" so it is relevant & the user doesn't have to answer unnecessary questions.

By asking employees contextual questions – and linking their answers immediately against the rules database – the tool not only guides, but educates the employee on good privacy practices. For each question, terms are defined by using text rollovers and help is provided that links the employee directly into the HP Privacy Rulebook. They can also check a box that says "Question is Unclear." This allows the Privacy Office to track trends and improve the delivery of questions if patterns evolve.

The tool takes the employee through a series of questions related to the profile and nature of the project, data sources and flows, transparency, compliance, and indicators of any issues that might arise or surprise the data subject. Once the employee has completed the questions, a report is generated that shows an overall rating, as well as areas of compliance and non-compliance.

Assessment Report

Project Information

This section provides details of the project.

Leading Organization: PSG Asia Pacific & Japan
Leading Business Unit: Emerging Markets (PSG)
Leading Business Group: Personal Systems Group-PSG
Project/Campaign Region: Asia Pacific
Project Lead: Allan Paull
Lead Email: allan.paull@hp.com
Owner Name: Allan Paull
Owner Title: null
Owner's Phone: +61 411 232 249
Owner's E-mail: allan.paull@hp.com
Edited by: allan.paull@hp.com

Summary Of Findings



eMail marketing campaign test has been found to be **compliant** by the HP Privacy Account. Please contact the Privacy Office if you would like to discuss any related issues.

Summary of findings

Risk Indicators

Risk indicators graph

This graph shows the number of green, yellow and red flags triggered for each risk indicator.

For areas of non-compliance, reasons are provided, including links to further information and checklists that can be used to achieve compliance.

Detailed information per risk indicator



A. Transborder data flow

The following low risks have been identified:



B. HP compliance/Non-compliance

The following low risks have been identified:



C. Other

The following moderate risks have been identified:



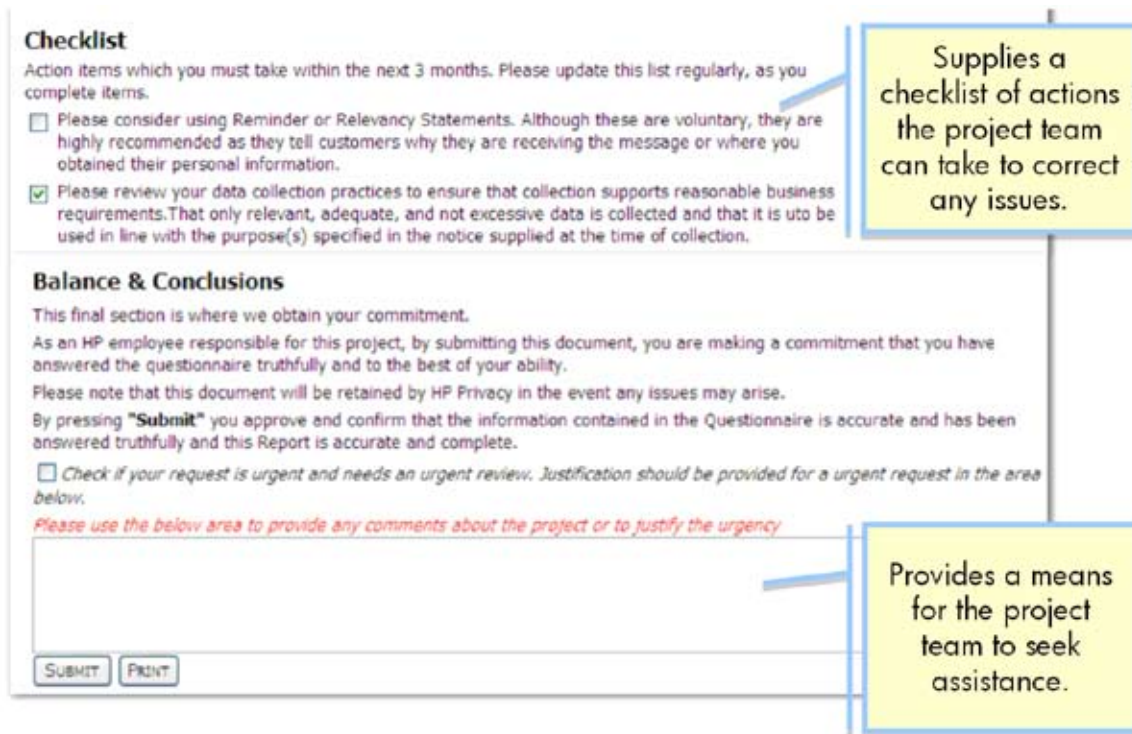
Relevancy statements are highly recommended, but not required. Relevancy Statement: Tell customers why they are receiving the message or where you obtained their personal information. Can appear in the introduction, body, or footer of the message; recommended placement is in the introduction.

- One-to-One Sales: In response to your request
- One-to-One Transactional: You are receiving this message because you reported an issue to our call center
- One-to-Many Marketing: You are receiving this message because it matches your current subscription profile
- One-to-Many Transactional: In response to your request. You are receiving this message as part of your service agreement with HP
- Joint Marketing: You are receiving this advertisement from HP and [insert partner name] because HP and [insert partner name] offer complementary solutions that match the interests

[View details](#)

Details of compliance & non-compliance

Once the employee has made the appropriate modifications, he or she can submit their report to the HP Privacy Office where it will be reviewed and archived.



Checklist
Action items which you must take within the next 3 months. Please update this list regularly, as you complete items.

- ☐ Please consider using Reminder or Relevancy Statements. Although these are voluntary, they are highly recommended as they tell customers why they are receiving the message or where you obtained their personal information.
- ☒ Please review your data collection practices to ensure that collection supports reasonable business requirements. That only relevant, adequate, and not excessive data is collected and that it is used in line with the purpose(s) specified in the notice supplied at the time of collection.

Balance & Conclusions
This final section is where we obtain your commitment.
As an HP employee responsible for this project, by submitting this document, you are making a commitment that you have answered the questionnaire truthfully and to the best of your ability.
Please note that this document will be retained by HP Privacy in the event any issues may arise.
By pressing "Submit" you approve and confirm that the information contained in the Questionnaire is accurate and has been answered truthfully and this Report is accurate and complete.

☐ Check if your request is urgent and needs an urgent review. Justification should be provided for a urgent request in the area below.

Please use the below area to provide any comments about the project or to justify the urgency

Callouts:

- Supplies a checklist of actions the project team can take to correct any issues.
- Provides a means for the project team to seek assistance.

They are attesting to the truth and accuracy of their statements and will be held accountable. For any areas of concern, the Privacy Office must approve the program prior to deployment.

Once approved, the program information is warehoused in the database. It is maintained for future use as well as a trigger for ongoing assurance monitoring. This database of projects provides a real-time dashboard for the Privacy Office, allows improved ongoing communications and ensures that if laws or regulations in a country change that programs can be modified as appropriate.

This is a new program for HP and has just been deployed. It is a valuable tool along with ongoing efforts in training, implementation standards, compliance management, and audit. It achieves Commissioner Cavoukian's concepts for *Privacy by Design* in a manner that is systematic, predictable and repeatable – and ultimately will drive a richer culture of privacy within the enterprise. It also will enable HP to better demonstrate commitment and capacity in upholding privacy promises and obligations.

VI Conclusion

In this paper, we have seen an excellent example of how enhanced privacy accountability and assurance can be achieved within an organization by applying *Privacy by Design* principles, in a thoroughgoing manner.

So imperative today are the goals of enhanced accountability and assurance, so universal are the PbD principles, and so diverse are the contexts within which these principles may be applied, that the future of privacy in the 21st century information age may be limited only by our collective imagination and will.

There are virtually infinite ways by which organizations can creatively “build privacy in” to their operations and products, to earn the confidence and trust of customers, business partners and oversight bodies alike, and to be leaders in the global marketplace.

We need to acknowledge and celebrate these innovations and successes, and steadily build upon them.

About the Authors

Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

Martin E. Abrams, Senior Policy Advisor and Executive Director, Centre for Information Policy Leadership, Hunton & Williams LLP

Martin Abrams is Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP, a global privacy and information security think tank, and an advisor to the Business Forum for Consumer Privacy. Mr. Abrams brings more than 30 years' experience as a policy innovator to the Centre, where he pursues practical solutions to privacy and security problems. He is a leading theorist on global transfers of data based on accountability, and has led the movement in the U.S. to adopt harms-based approaches to privacy. He was a leader in developing layered privacy notices, and is currently working to bridge cultural differences in privacy. Mr. Abrams has led privacy programs on five continents, and is part of the APEC Data Privacy Subgroup.

Scott Taylor, Chief Privacy Officer, Hewlett-Packard Company

As head of HP's privacy and data protection efforts worldwide, Scott Taylor is responsible for global privacy strategy, policy, governance, and operations. In this role, he is a member of HP's Ethics & Compliance Council, Global Citizenship Committee, and chairs HP's Privacy & Data Protection Governance Board. Taylor and his team work with HP business groups, regions and corporate functions to assure the implementation of HP's privacy policies and programs and integrate privacy into product and services development across the company. He serves as HP's global representative with external policy-makers, media, NGOs and customers in the area of privacy and data protection. Taylor serves on the Board of Directors for The Business Forum for Consumer Privacy, as the Chairman of the Executive Council at The Center for Information Policy Leadership, and on the Board of Directors for the Council of Better Business Bureaus. Taylor has been with HP for 22 years. Previously he led HP's global Internet program, part of the Global Operations Organization. In that role, he and his team handled Internet strategy, customer experience, e-business policies, standards, worldwide site management, and operations. Taylor led the team that launched HP's Internet presence in 1994 and managed it for 12 years. Prior to that, Taylor was responsible for HP's direct marketing function, part of the Corporate Marketing & International Services Organization.



Information and Privacy Commissioner of Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario M4W 1A8
Canada
Telephone: 416-326-3333
Fax: 416-325-9195
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

The Centre for Information Policy Leadership

at Hutton & Williams LLP
1900 K Street, NW
Washington, DC 20006
USA
Telephone: 202-955-1500
Fax: 202-778-2201
Website: www.informationpolicycentre.com

Hewlett-Packard (Canada) Co.

5150 Spectrum Way
Mailstop 6H72
Mississauga, Ontario L4W 5G1
Canada
Telephone: 905-206-4725
Fax: 905-206-4739
Website: www.hp.ca

The information contained herein is subject to change without notice. HP, CIPL - Hutton & Williams, LLP, and IPC shall not be liable for technical or editorial errors or omissions contained herein.



World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 10, Number 10

October 2010

Accountability: Part Of The International Public Dialogue About Privacy Governance

By Paula J. Bruening, Centre for Information Policy Leadership at Hunton & Williams LLP, Washington.

Dramatic advances in the speed, volume and complexity of data flows challenge existing models of data protection. Powerful analytics yield deeply insightful, real-time inferences about computer users that enhance the online experience and enable companies to offer products and services to the right individual at the right time. Behavioral targeting uses a complex network of vendors to track and analyze an individual's online activity to serve tailored, more effective advertising. Organizations collect and derive data about individuals from myriad sources and often employ service vendors located halfway around the world to carry out internal business processes and provide around-the-clock customer service. Using technologies ranging from surveillance cameras to radio frequency identification, they gather and store data cheaply, often in the cloud, where servers may be located on another continent. And given the rapid pace of development, an organization's impulse to retain that information for future, as yet unanticipated, uses is understandable and often makes good business sense.

The growing power of data holds the promise of economic benefit for businesses and consumers. But to realize that potential, consumers must be confident that their information is used responsibly, and that their privacy is protected. Over the last 18 months, policy-

makers around the world have undertaken efforts to examine and update data governance in a way that would better serve this rapidly changing data environment, providing the best possible privacy protection while encouraging innovation and flexible data use. While policymakers continue to cite traditional principles of fair information practice as relevant and the foundation of good privacy and data protection, they recognize the challenges new technologies and business models pose to the application of those principles.

Data protection that relies primarily on notice and choice has come under particular scrutiny. In a notice-and-choice model, consumers receive information about how an organization will collect, use, and share data about them. On the basis of this notification, consumers choose whether to allow its use. Such a model is seriously challenged by an environment in which organizations can analyze and process information instantaneously at the collection point, and where data collection has become so ubiquitous that individuals could easily be overwhelmed by the privacy notices they receive each day as they shop online, use a mobile communications device, engage in social networking, or visit a building that uses surveillance cameras or sensor technology. In many cases, it is impossible to provide notice, and even when it is, notices are lengthy and complex. Given that data use is necessary for so many activities, both online and offline, choice itself

may be possible and provide real guidance for organizations about how to use information only in limited circumstances.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed.

Faced with these challenges, policymakers are asking a number of questions. How best to protect the privacy of individuals, even when choice is not meaningful or in some instances not possible? How to encourage the innovation in data use that encourages economic growth and still safeguard individuals' interests in the protection and responsible use of their data? For possible answers, policymakers have turned their attention to the fair information practice principle of *accountability*.

Accountability as a principle of data protection is not new. It was first articulated in 1980 as a principle of fair information practices in the Organization for Economic Cooperation and Development's (OECD) privacy guidelines.¹ The accountability principle places responsibility on organizations as data controllers "for complying with measures that give effect" to all eight of the OECD guidelines' principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly articulated in the EU Data Protection Directive (95/46/EC), numerous provisions require that organizations 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. It is the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),² which requires that Canadian organizations implement the full complement of PIPEDA principles, whether the data are processed by the organization or outside vendors, or within or outside Canada. In the United States, accountability underpins the security requirements of the Gramm-Leach-Bliley Act, which requires that organizations secure their data holdings against theft, loss or unauthorized access, but leaves to their discretion the most effective way to do so.

Accountability Project

Until now, the principle of accountability has often gone undefined, and it has been unclear what conditions organizations must create to establish and demonstrate their accountability. As it has begun to play an increasingly visible role in privacy governance, an international group of experts — including business leaders, data protection authorities, advocates, and government representatives — have convened the Accountability Project. Organized by the Centre for Information Policy Leadership, the Accountability Project seeks to define the contours of accountability, to articulate how it is demonstrated and measured, and to establish why individuals should trust it to protect their data. Their work began as

an inquiry into the essential elements of accountability in early 2009, and will continue into 2011 to more concretely define the fundamentals that characterize the accountable organization.

According to the Project, accountability is designed to provide robust protections for data while avoiding aspects of current data protection that may be of limited effect or that may burden organizations without yielding commensurate privacy benefits. Accountability allows the organization greater flexibility to adapt its data practices to serve emerging business models and technologies and to meet consumer demand. In exchange, it requires that the organization commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a way that protects information and the individuals to which it pertains.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed. An accountability-based approach to data governance focuses on setting privacy-protection goals for organizations based on criteria established in current public policy and allowing organizations discretion in determining how those goals are met. Accountable organizations will adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the demands of their customers.

The essential elements of accountability are:

1) Organization commitment to accountability and adoption of internal policies consistent with external criteria

An organization demonstrates its willingness and ability to be responsible and answerable for its data practices. Its practices are based on policies consistent with appropriate external criteria — applicable law, generally accepted principles, and/or industry best practices. Practices are designed to provide the individual with effective privacy protection.

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

The accountable organization deploys and monitors mechanisms and internal programs that ensure its privacy policies are carried out. Mechanisms may include tools to facilitate decision making about data use and protection, training about how to use those tools and processes to ensure employee compliance.

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

The organization monitors and assesses whether its internal policies manage, protect and secure data effectively. Risk analysis appropriate to the organization and the industry in which it functions is key to successful monitoring and risk management. The accountable organization engages, as appropriate, an independent entity to verify and demonstrate that it meets the requirements of accountability.

4) Transparency and mechanisms for individual participation

Accountability requires transparency. The accountable organization effectively communicates to indi-

viduals critical information about its data procedures and protections in a posted privacy notice. When appropriate, the information in the privacy notice can provide the basis for the consumer's consent or choice. Individuals should be able to see the data or types of data that the organization 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. In some cases, however, public policy reasons will limit that disclosure.

5) Means for remediation and external enforcement

The accountable organization establishes a means to address harm to individuals caused by the failure of internal policies and practices. When harm occurs due to a failure of an organization's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. The organization should identify an individual to serve as the first point of contact for resolution of disputes and establish a process to review and address complaints.³

Developers envision the ability of an accountability approach to improve data protection in several ways. Ideally, accountability will:

- help organizations 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 respond quickly to new business models and emerging technologies;
- enable organizations to better deploy scarce resources allocated to privacy protection. Resources devoted to administrative requirements such as notification of data authorities of minor changes in processing can be redirected to more effective protection measures that most effectively safeguard data;
- heighten the confidence of individuals that their data will be protected wherever it is stored or processed; and
- bridge data protection regimes across jurisdictions, but allow countries to pursue common data protection objectives through very different but equally reliable means.

Accountability does not preclude application of principles of fair information practices. It does relieve the individual of much of the burden of policing the marketplace for organizations 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. In an accountability model, when the consumer can provide meaningful consent, the organization is required to act based on that consent. But even when the consumer cannot, accountability demands responsible, disciplined data storage, use and protection.

Factor in International Discussions

Accountability has begun to figure prominently in ongoing discussions about effective data protection.

Accountability has come under close review in the European Union. The Article 29 Working Party launched a consultation on the EU data protection legal framework and determined that the level of data protection in the European Union could benefit from better application of existing data protection principles in practice. In an article released in December 2009 entitled "The Future of Privacy,"⁴ the Article 29 Data Protection Working Party and the Working Party on Policy and Justice noted that, while traditional principles of data protection remain valid, new technologies and the global flow of data present new challenges to data protection. They characterized the new challenges as an opportunity to, among other things, introduce additional principles, including accountability. It also noted the need to strengthen the effectiveness of the current system through modernization, citing particularly the need to reduce bureaucratic burdens.

In July 2010, the Article 29 Working Party released an opinion focusing specifically on accountability⁵ (*see analysis in this issue*). According to the opinion, a principle of accountability "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the [Data Protection] Directive and demonstrate this on request." The Working Party's objective is to "encourage data protection in practice" by requiring data controllers to engage in risk assessment and adopt measures such as:

- data loss/breach detection/prevention policies and procedures;
- "Privacy by Design" in the development and implementation of new technologies;
- binding policies and procedures that measure compliance; and
- response plans that draw on the organization's experience, mitigate harm and discourage future breaches.

At the Asia-Pacific Economic Cooperation, the Privacy Framework⁶ depends upon accountability to facilitate cross-border data flows. In language similar to that in the OECD Guidelines, the APEC Framework provides that "[a] personal information controller should be accountable for complying with measures that give effect to the Principles stated above."

The Framework commentary specifically discusses accountability in the context of information transfers between different types of organizations, in different locations. It states that controllers should be accountable for ensuring that the recipient of the information will protect it in accordance with the Framework principles. Under the APEC Framework, controllers are accountable for protection of the data even after it is transferred for processing or storage. The requirement assumes that the controller will conduct due diligence to ensure that the recipient is able and committed to fulfilling the obligations to manage and protect the data appropriately.

Finally, the proposed "International Standards on the Protection of Personal Data and Privacy" that are the subject of the Madrid Resolution⁷ also incorporate the

principle of accountability. The principle recognizes both the obligation to observe all of the principles and obligations in the proposed standard, and takes the additional step to require that organizations implement mechanisms and be able to demonstrate their compliance.

Summary

Accountability has become part of the international public dialogue about privacy governance. But to be an effective, credible solution to the privacy issues raised by 21st century data use, it will be necessary to establish the fundamentals that would make an accountability model work in practice.

The Accountability Project is engaged in additional collaborative work to explore the practical questions related to implementing and administering an accountability approach. What must an organization demonstrate to be deemed accountable? How is accountability measured? What triggers an accountability review? How will remediation work in an accountability approach?

Resolution of these and other questions by international policymakers, business, experts and advocates will be critical to accountability's successful adoption as an innovative, effective approach to privacy and data protection.

NOTES

¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

² <http://laws.justice.gc.ca/en/P-8.6/>

³ For a more comprehensive discussion of accountability, see "Data Protection Accountability: A Document for Discussion," October 2009, <http://www.ftc.gov/os/comments/privacysummarytable/544506-00059.pdf>.

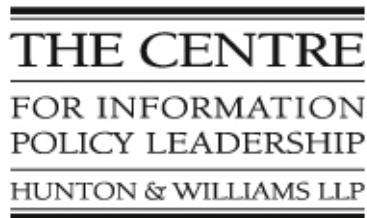
⁴ "The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data." 02356/09EN/ WP 168, December 1, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

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

⁶ The APEC Privacy Framework, published 2005, <http://op.bna.com/pl.nsf/r?Open=byul-89js2b>

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>.

Paula J. Bruening is Deputy Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP in Washington. She may be contacted at pbruening@hunton.com.



HUNTON & WILLIAMS LLP
1900 K STREET, N.W.
WASHINGTON, D.C. 20006-1109

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

PAULA J. BRUENING
DIRECT DIAL: 202 • 955 • 1803
EMAIL: PBRUENING@HUNTON.COM

February 28, 2011

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899-1000

**Re: Guidelines on Security and Privacy in Public Cloud Computing
Draft Special Publication 800-144**

Dear Sirs and Madams:

The Centre for Information Policy Leadership (the Centre) appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) recently released "Guidelines on Security and Privacy in Public and Cloud Computing." The Centre commends NIST for undertaking work on this important issue.

The Centre's mission is development of forward-thinking information policy that encourages both privacy and innovation in a digital economy. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, development of privacy law in emerging economies and government's use of private sector data. The Centre currently serves as secretariat for an international project to describe an accountability approach to data management and protection that would facilitate innovative data use and robust data flows, while fostering strong security and privacy protections. The Centre has worked extensively with businesses, advocates, experts, congressional staff and international organizations on issues of privacy and data protection.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. It is located within the law firm of Hunton & Williams and is financially supported by approximately 40 member organizations. 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 firms' clients.

National Institute of Standards and Technology

February 28, 2011

Page 2

In commenting on the Guidelines, the Centre acknowledges their orientation to public cloud computing and their recommendation to departments and agencies of the United States federal government. While its work in this area has focused primarily on data in the private sector, the Centre recognizes that the Guidelines, while intended for application within government, may serve as a starting point for articulation of similar guidance and best practices for businesses and other private sector organizations. The Centre believes that it is important to consider them in that light.

The Guidelines suggest governance of data in the cloud based on accountability. While accountability is a well-established principle of data protection and is found in known guidance such as the OECD Guidelines¹ and the APEC Privacy Framework,² policymakers have only recently articulated how the principle is applied and adhered to, and how accountability is demonstrated or measured.³ The proliferation of data, the robust flows of data across borders, and organizations' need for flexible, protected data use to support the innovative business models and technologies that fuel economic growth have prompted efforts to define the contours of accountability.

As currently understood, an accountable organization is characterized as one that commits to accountability and implements data privacy policies linked to recognized outside criteria. It establishes mechanisms to ensure responsible decision-making about the management of data consistent with those policies. It assesses the risks raised by data use and mitigates them accordingly. Significantly, the obligations stated in those policies, as well as those in law and regulation, must be met no matter where or by whom the data is processed. In an accountability

¹ Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Data Flows, Principle 8, Accountability, 1980.
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last accessed February 23, 2011).

² APEC Privacy Framework, Principle 9, Accountability, was endorsed by APEC ministers 2004.
http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF (last accessed February 23, 2011).

³ Policymakers are examining accountability and its practical application in data governance through the Accountability Project (convened in Galway, Paris and Madrid), an international process that began in 2009. For a thorough discussion of accountability and the findings of that project, see "Data Protection and Accountability: The Essential Elements," published October 2009 and available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last accessed February 23, 2011). See also "Demonstrating and Measuring Accountability," published 2010 and available at http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF (last accessed February 23, 2011).

National Institute of Standards and Technology

February 28, 2011

Page 3

approach, custodians of data would remain responsible for securing the data and meeting privacy requirements, even when it is processed in the cloud.

The NIST Guidelines reflect several aspects of an accountability approach. Accountability requires that organizations put in place programs and mechanisms to foster adherence to data protection requirements. The Guidelines facilitate that implementation by recommending that the security and privacy elements of cloud computing be considered and addressed early in the effort to transition data processing activities.

It is well accepted that privacy and security issues related to any new technology, business model or data use are best contemplated in the earliest stages of development and that means to address those risks be considered and incorporated appropriately throughout the development process. Often referred to as “privacy by design,” this approach encourages organizations to take active steps to address privacy at the outset, and to embed mechanisms to protect data into all aspects of the design of the new initiative. Privacy impact assessments may serve as a first step, whereby organizations review and analyze the risks a new product, service or data use might raise, and consider the means available to mitigate those risks

As NIST notes in the Guidelines, by building in appropriate privacy and security measures from the beginning, organizations gain a realistic understanding of their data holdings and activities, and can take steps throughout the development process to implement optimal protections. By incorporating privacy and security into processes and procedures, organizations can reap the benefits of more cost-effective, streamlined solutions than when protections are added on to a final product or process.

An accountability approach is further suggested in the Guidelines’ recommendation that organizations review cloud computing solutions to ensure that they are “configured, deployed, and managed to meet their security, privacy, and other requirements.”⁴ They recommend similar due diligence regarding the client-side computing environment for cloud computing. When data is governed by an accountability approach, organizations are required to protect and secure it no matter where or by whom it is maintained or processed. Organizations must be sure that the obligations that pertain to data -- whether in law, regulation, industry best practices or promises made to the consumer -- can be honored. While additional measures may be required to provide the necessary assurances, the review recommended in the Guidelines represents one tool organizations can use to ensure that the data is appropriately protected in the cloud.

⁴ Privacy and security heavily depend on whether the cloud service provider has implemented robust security controls and a sound privacy policy, the visibility that customers have into its performance, and how well it is managed by users.

National Institute of Standards and Technology

February 28, 2011

Page 4

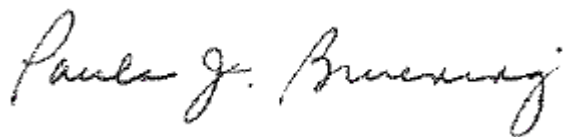
The Guidelines encourage risk analysis and mitigation to determine whether security and privacy controls are implemented correctly, operate as intended and meet necessary requirements. Accountability relies on an organization's understanding of the risks raised by data use, and the organization's efforts to mitigate those risks. Such analysis forms the basis for decisions about how data may or may not be used, and what measures should be taken to be sure that it is managed and secured in accordance with law, regulation, best practices and organization policies. It serves as the foundation for determining what kinds of controls should be put in place to effectively address the risk, and how the data should be secured.

Finally, the Guidelines suggest that organizations assess the effectiveness of security and privacy controls. It recommends "assessing the implementation of policies, standards, procedures and guidelines that are used to establish and preserve the confidentiality, integrity, and availability of information system resources." Accountability similarly requires such internal review to ensure that security and privacy controls are implemented correctly, operate effectively and result in sound decision-making about data use and protection.

The Centre is encouraged by NIST's adoption of such forward-thinking guidance. The Guidelines affirm an organization's continuing responsibility for data security and privacy when stored and processed in the cloud. NIST's recommendations acknowledge growing recognition that innovative data processing requires that organizations be accountable for responsible decisions about data protection wherever and by whomever it is processed. As policymakers continue to address questions of security, privacy and management in the cloud, this guidance serves as a useful foundation for thoughtful, effective data practices.

The Centre appreciates the opportunity to comment on the Guidelines. It is available to discuss these comments further, and would be pleased to serve as a resource to NIST as it continues to work on security and privacy guidance for emerging information technologies.

Respectfully submitted,

A handwritten signature in dark ink, reading "Paula J. Bruening". The signature is written in a cursive, flowing style.

Paula J. Bruening
Deputy Executive Director



HUNTON & WILLIAMS LLP
1900 K STREET, N.W.
WASHINGTON, D.C. 20006-1109

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

MARTIN E. ABRAMS
DIRECT DIAL: 202 • 778 • 2264
EMAIL: MABRAMS@HUNTON.COM

PAULA J. BRUENING
DIRECT DIAL: 202 • 955 • 1803
EMAIL: PBRUENING@HUNTON.COM

February 18, 2011

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue
Washington, DC 20580

Re: “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers”

Dear Sirs and Madams:

The Centre for Information Policy Leadership appreciates the opportunity to respond to questions posed in the Federal Trade Commission (“FTC”) preliminary report, “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.” The Centre commends the FTC for undertaking work on this important issue.

The Centre’s mission is development of forward-thinking information policy for a digital economy that encourages both privacy and innovation. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, accountability-based governance, development of privacy law in emerging economies, and government’s use of private sector data. The Centre has worked extensively with business, advocates, experts, congressional staff and international organizations on issues of privacy and data protection. In responding to the questions posed in the FTC preliminary report, the Centre focuses on areas where it has actively engaged in research and policy development.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. It is located within the law firm of Hunton & Williams and is financially supported by approximately 40 member organizations. 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.

Federal Trade Commission
February 18, 2011
Page 2

Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

The Centre agrees that organizations should incorporate into their data practices the privacy protections cited by the FTC in Section V(B)(1) of the report -- data security, reasonable collection limits, sound retention practices and data accuracy. The Centre further agrees that these protections should be implemented as part of data governance that applies a comprehensive set of fair information practices. The Centre believes that organizations should be accountable for implementation of internal processes that ensure these protections are in place and that its practices are adhered to.

An accountable organization develops data management and protection policies that correspond to recognized external criteria, such as the OECD Guidelines or the APEC Privacy Framework. It puts in place programs and mechanisms that implement those policies and measure their effectiveness. It bases its decisions about data management on credible assessment of the risks the use of data may raise for individuals, and judgments about whether those risks can be adequately mitigated. It responds to regulatory oversight, and provides a means for remediation for individuals.¹

Principles of fair information practices are applied flexibly in an accountability approach. They are applied in a contextual framework in which different principles carry more importance depending on the nature of the data, its sensitivity, or how it is used. The FTC's proposed framework raises questions about whether it may be possible "to prescribe a reasonable retention period[.]" The report asks whether the definition of "specific business purpose" or "need" can be further refined. While increased clarity is desirable, in the current environment it is important to guard against application of bright-line definitions. Data today proliferate rapidly and are collected from consumers in places and in ways not anticipated even five years ago. The current environment of fast-paced innovation in technology requires that organizations are positioned to respond quickly to the market. An accountability approach allows for flexible use of data that meets those needs but requires responsible decisions about management of information that protects individual privacy. Such flexibility is ideally balanced with FTC guidance

¹ For further discussion about accountable organizations, see "Demonstrating and Measuring Accountability: A Discussion Document," prepared by the Centre as secretariat to the Accountability Paris Project, published October 2010. See Appendix A and http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF (Last accessed February 17, 2011).

Federal Trade Commission
February 18, 2011
Page 3

about how principles are best applied, and safe-harbor protections for organizations that comply with the guidelines.

For example, authentication and fraud prevention require collection of sensitive information to predict risk and to identify legitimate and rogue entities who may wish to access systems. Application of the principle of collection limitation may be applied to each with equal rigor, but to different effect. Given the potential sensitivity of identifying information, an organization would be expected to implement security in a manner that addresses the risks raised by the collection, use and retention of that information. In an accountability approach, rather than comply with prescriptions that may not serve the breadth of data use, the organization would make such an evaluation based on its assessment of the risks data use raises for individuals, and apply the principle of collection limitation and security, as well as the other fair information practice principles, in accordance with its findings. The organization would then be answerable to regulators and to individuals for the soundness of the processes that led to those decisions.

How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

While many organizations already have implemented the accountability-based programs discussed above, companies adopting new policies and programs to manage and protect information will require a phase-in period to apply those systems and processes to legacy data. Decisions about how this phase-in is carried out and how much time it will require will be based on public policy, business judgments, and industry considerations. The sensitivity of the information, the nature of the use, the risks raised and the extent to which they can be mitigated will all factor into decisions about how new systems will be applied to legacy data. In some cases, legacy systems may have to be completely replaced before all of the principles can be applied.

Further, it will be important to evaluate the phasing in of new safeguards in light of how well existing legacy system processes and programs perform with respect to privacy. In some cases, existing protections may provide adequately for privacy and can be phased out as new protections are developed and implemented. Doing so would maintain appropriate safeguards and avoid placing unnecessary burdens on companies that have not experienced privacy failures.²

² The Centre does not suggest changes to the requirements of existing consumer protections such as those found in the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.) or in the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (45 CFR Part 160 and Part 164, subparts A, E).

Federal Trade Commission
February 18, 2011
Page 4

How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

Privacy-enhancing technologies may serve as one measure in the comprehensive approach to accountable data management and protection discussed earlier in these comments. The FTC cites several privacy-enhancing technologies. Data tagging tools enable collectors and processors to understand and comply with requirements in law and policy that apply to information.³ Encryption technologies enhance data security. And identity management ensures that only authorized individuals can access information, systems and networks. Such tools all represent measures that can be taken by organizations to manage and protect data. In an accountable organization, decisions about which tools may be appropriate will be based on credible risk assessment and an evaluation of which will yield optimal privacy results.

The market will provide organizations with some incentives to deploy privacy-enhancing technologies and broader accountability measures. Such organizations will enjoy enhanced recognition by consumers for responsible data practices and responsiveness to individuals. Organizations that adopt comprehensive data management procedures will also lower their risk of compromise to data, and the attendant exposure to legal liability and compromise to brand and reputation.

Regulators can also provide incentives. Safe-harbor protections would provide strong incentives for organizations to develop and deploy data management and protection programs. Regulators also must apprise organizations of effective negative incentives for non-compliance.

What is the most important way to obtain consent for practices that do not fall within the “commonly accepted” category?

What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

³ Bruening, P. J. and Krasnow-Waterman, K., “Data Tagging for New Information Governance Models,” *IEEE Security and Privacy*, vol. 8, No. 5, September/October 2010. See Appendix B and http://www.hunton.com/files/tbl_s47Details/FileUpload265/2956/Data_Tagging_Bruening.pdf (Last accessed February 18, 2011).

Federal Trade Commission
February 18, 2011
Page 5

As the FTC's questions related to improving consumer choice and enhancing transparency are related, we address them together.

A transparency plan is fundamental to privacy-by-design⁴ or accountability. A transparency plan includes notice, stated policies, and educational materials (*e.g.*, tutorials, frequently asked questions, and video presentations) that help the consumer understand how information is used within an organization and among its business partners and service providers. A transparency plan may also include the organization's adherence to industry codes of conduct and education materials that raise consumer awareness.

In practically addressing the need to increase transparency of data practices, the FTC should be mindful of the goal of transparency: to make visible the information policies and practices that are important to the individual. Thus, the data activities that should feature most prominently in an organization's transparency plan are those that are the most important to the individual, either because they raise significant risks or because the reasonable individual would not anticipate them. Activities such as those identified by the FTC as being generally accepted -- including fulfillment, payment, and first-party marketing -- would be given less prominence in an organization's transparency plan.

Transparency makes it possible for individuals to exercise choice, when choice is available to them. It may affect the decisions individuals make about with whom they choose to do business. It enables observers of data practices in the marketplace (*e.g.*, policymakers, press and advocates) to identify activities they may believe inappropriate and that may require some kind of response by companies, individuals or regulators. In doing so, transparency fosters a fair and informed market.

Individuals' ability to access data pertaining to them enhances transparency. That access may be to the information itself; or it may be to a description of the kinds of information about them an organization collects and maintains. It facilitates the individual's awareness of what and how data about him or her is collected, processed and retained. It also promotes the accuracy and quality of data and its suitability for a specific purpose. However, the way access is provided should be based on the risks raised by the

⁴ The Centre acknowledges the importance of Commissioner Cavoukian's work on concepts of privacy-by-design. (Martin Abrams of the Centre and Scott Taylor of Hewlett Packard collaborated with the Commissioner in 2009 on "Privacy-by-Design: Essential for Organizational Accountability and Strong Business Practices.") However, the Centre suggests that for purposes of regulatory oversight and industry compliance, the FTC will need to further define the contours and requirements of privacy-by-design. The Centre offers its resources and looks forward to working with the FTC as it embarks upon that effort.

Federal Trade Commission
February 18, 2011
Page 6

sensitivity of the data and the way it is used. When information forms the basis for substantive decisions about the individual, he or she should have full access to the contents of the file and the right to challenge or correct the data where appropriate.⁵ In instances where data is not essential to making decisions about the individual, access might involve providing a detailed description of the types of data pertaining to him that the organization collects, uses, and stores.

Notice is one aspect of an organization's transparency plan, and determining how best to deliver notice of an organization's data management and policies has proven troublesome in both the on-line and off-line environment. How does a retailer deliver notice at point-of-sale in a brick-and-mortar store? How can a notice effectively communicate pertinent information on a hand-held wireless device? How can notice be delivered online in a way that provides critical information but does not interrupt the user experience or slow the transaction?

Obligations for delivering notice must correspond to what can reasonably be achieved. However, the fact that providing effective notice is challenging does not mean that it is not an effort worth undertaking. For example, while it is still unclear how to provide notification on the Internet without interfering with the user experience, it remains important to continue to work toward notices that serve the individual and the organization in those circumstances.

Resolving the question of notice will require the same innovative skill and energy that is brought to the development of new business models and digital technologies. To foster an environment where organizations will attempt new mechanisms for notice that approach the dual goals for transparency, the FTC will need to provide guidance for their development and safe harbor for their implementation. Doing so will enable organizations to deliver notice messages based on the risks data raises for individuals and the extent to which its use deviates from commonly accepted practices. Failure to provide such protections will prove a disincentive to any effort to tailor notices to deliver pertinent information succinctly and meaningfully.

Finally, the FTC asks how companies might best obtain consent for practices that "do not fall within the 'commonly accepted' category" set forth in its report. The Centre cautions that the categories noted in the document as "commonly accepted" business practices not be interpreted in a static or rigid way. Given the dynamic nature of information use and

⁵ The provisions of the Fair Credit Reporting Act describe instances in which data forms the basis for substantive decision-making about individuals. 15 U.S.C. Section 1681b (a) (3).

Federal Trade Commission
February 18, 2011
Page 7

technology development, it will be important to view business practices in context. In some areas of business and data use, a certain practice may be commonly accepted, while in others that same practice may not.⁶ It will be important to engage in an open process to provide clearer guidance about what would be deemed to fall into this category. Moreover, safe harbor protections for those who adhere to such guidelines would provide incentives for compliance.

Should companies be able to charge a reasonable cost for certain types of access?

In some settings, charging for access is appropriate. Individuals accessing specific data about themselves may be required to pay a fee, while those obtaining a general report about the types of data about themselves the organization maintains would not. Any fee should also reflect the difficulty associated with retrieving data and providing it to the consumer in a meaningful way. Access to data that is brought together from several locations and that must be reformatted so that the individual can understand it, therefore, would cost more than access to data that is more readily available. Companies might charge individuals less to see data about them that is accessed in the ordinary course of business.

Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

Whether companies should inform consumers of the identity of those with whom they have shared data depends upon the circumstances. Industry rules⁷ require that marketers, when asked by the consumer, identify the data supplier. Because marketers have direct contact with consumers, their data systems are structured so that the marketer can accommodate this transparency requirement. While suppliers of marketing and lists and enhancement data know the identities of their client companies to which they supply lists and enhancement, they are not structured to correlate that marketing information to the individual to whom the data pertains. To do so would require fundamentally changing systems and likely would yield only a marginal change in the transparency about marketing data. The utility of requiring fundamental changes to systems that would result in only a slight increase in transparency is questionable.

⁶ For example, when organizations collect and maintain sensitive information about individuals, such as for banking or issuance of credit, they will ask for authenticating information before an individual can access those records. Organizations holding less sensitive data may not require similarly rigorous authentication.

⁷ See the Direct Marketing Association's *Guidelines for Ethical Business Practices*, p. 19, <http://www.dmaresponsibility.org/guidelines/>, last accessed February 17, 2011.

Federal Trade Commission
February 18, 2011
Page 8

Consumer education

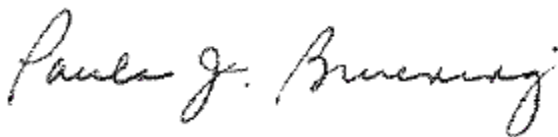
Consumer education related to privacy should be an ongoing effort of business, advocates and government. Consumer education enhances transparency by helping individuals better understand privacy notices, when choice may be an option, and when access may be available to them. Taken more broadly, consumer education can also help individuals gain a better understanding of evolving data practices and uses, and how the use of information can both provide benefits and raise risks to individuals. Because individuals may not seek out information independently, stakeholders should identify opportunities -- online and through other outlets -- to give individuals the appropriate, necessary information that will increase their understanding of data practices and their familiarity with the steps they can take to actively participate in protecting their privacy. Such efforts will require focused attention and increased funding from both government and industry.

The Centre commends the FTC on its leadership in addressing these timely and complex issues, and particularly for the open and public series of workshops that informed the drafting of the proposed framework. It appreciates the opportunity to participate in the process and to submit these comments. The Centre is available as a resource to the FTC as it continues this important work.

Respectfully submitted,



Martin E. Abrams
Executive Director



Paula J. Bruening
Deputy Executive Director

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP

HUNTON & WILLIAMS LLP

HUNTON & WILLIAMS LLP
1900 K STREET, N.W.
WASHINGTON, D.C. 20006-1109

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

MARTIN E. ABRAMS
DIRECT DIAL: 202 • 778 • 2264
EMAIL: MABRAMS@HUNTON.COM

PAULA J. BRUENING
DIRECT DIAL: 202 • 955 • 1803
EMAIL: PBRUENING@HUNTON.COM

January 28, 2011

Office of the Secretary
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

Re: Docket No. 101214614-0614-01

“Commercial Data Privacy and Innovation in the Internet Economy: A
Dynamic Policy Framework”

Dear Sirs and Madams:

The Centre for Information Policy Leadership (“the Centre”) appreciates the opportunity to respond to questions posed in the Department of Commerce (“the Department”) Internet Policy Task Force document, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.” The Centre commends the Department on the release of its policy framework and on undertaking this important effort.

The Centre’s mission is development of forward-thinking information policy for a digital economy. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, accountability-based governance, development of privacy law in emerging economies, and government use of private sector data. The Centre has worked extensively with business, advocates, experts, congressional staff and international organizations on issues of privacy and data protection.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. It is located within the law firm of Hunton & Williams and is financially supported by approximately 40 member organizations. 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.

1. The Policy Framework should rely less upon the individual's control over the collection and use of data about him and more upon data stewardship and organizational accountability.

The Policy Framework proposed by the Department relies heavily upon a model based on the individual's ability to control the collection and use of data pertaining to him or her. This approach was anticipated when principles of fair information practices were originally articulated in the 1970s. In that early iteration, the principles were designed to provide individuals with sufficient information about how data about them would be collected, used, shared and stored. On the basis of that notification, individuals could choose whether to share data or to do business with an organization.

While individual control has traditionally motivated application of fair information practices, such an approach is no longer sufficient to protect individuals. The rate at which data proliferates today is vastly greater than it was in the 1990s, when the Internet emerged as a commercial medium. Data is collected from consumers in places and ways not anticipated even five years ago. Use of data about individuals has become so central to his or her ability to engage in basic life activities that choice may not always be an option. As the complexity of data collection practices, business models, vendor relationships and technological applications grows, it often outstrips the individual's ability to make decisions to control the use and sharing of information through active choice. While individual control remains important in some instances, such as when the data or the data use is sensitive or raises particular risks to individuals, control can no longer serve as the primary motivator of consumer privacy protection in every circumstance.

Moreover, the current environment of fast-paced innovation in technology and data applications is not well served by a control model. To be competitive, and to respond to consumer demand, organizations need to be able to use data in new ways, while still being responsible. A model that requires consent for each kind of data use may severely restrict organizations' ability to make decisions about data use that allow them to respond quickly to the market.

The Centre recommends that the Department consider instead an approach to data protection that relies upon organizations' accountability for the responsible management and protection of data. Accountable organizations implement mechanisms to ensure responsible decision-making about how data is optimally managed and safeguarded based on credible risk assessment. Such an approach requires that organizations commit to being responsible and answerable for their data collection and management decisions. They must put in place policies based on established external criteria and deploy mechanisms that implement those policies and measure their effectiveness.

Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing an increasingly complex, rapidly changing marketplace for enterprises using data irresponsibly. Accountability requires responsible data use whether or not a consumer has consented to one use or another. It also allows for flexible data use based on a realistic assessment and mitigation of the risks involved that enhances opportunities for innovation.¹

2. The Department should look to fair information practice principles as articulated in the OECD Guidelines as the foundation for privacy guidance.

The Centre agrees that in the current environment, application of a more comprehensive articulation of fair information practices is necessary to provide robust data protection. Adoption of a more complete set of fair information practice principles, while not an attempt to mirror other regimes, would create greater possibilities for interoperability with approaches in other regions. The Centre encourages the Department to adopt the OECD Guidelines² as the foundation for private sector guidance. Recognizing that guidance must keep pace with changes in technology, business processes and data applications, the Centre notes that the OECD Guidelines were developed in a technology-neutral way to encourage privacy, innovation and economic growth. There are numerous efforts under way to adapt the OECD Guidelines to respond to dramatic changes in information technologies and applications. The Department has helped lead one of the most successful as a part of its work on the Asia Pacific Economic Cooperative's Privacy Framework. The Centre is sponsoring another effort to fine-tune the OECD Guidelines to reflect the realities of 21st century data collection, processing and retention. (The attached discussion document by Professor Fred Cate, Senior Policy Advisor at the Centre, provides an introduction to that effort, and is intended to serve as a discussion platform within the Centre and with other stakeholders.) The OECD itself is now reviewing its Guidelines in a process in which the United States participates. We encourage the Department to look to these broader efforts.

3. Principles of fair information practices should be applied within a contextual framework, and not in a rigid or fixed way.

The Centre cautions against applying fair information practice principles inflexibly. Instead, they should be applied within a contextual framework in which different principles carry more

¹ An accountability approach is consistent with the framework on which the federal Fair Credit Reporting Act is structured and the manner in which bank regulators oversee data use governed by the Act. Both require that data collectors and users operate within a set of established legal requirements, and both place responsibility for appropriate data use and management on organizations rather than on individuals.

² The Organization for Economic Cooperation and Development issued its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

importance depending on the nature of the data, its sensitivity, or how it is used. For example, enhancing cyber security requires robust collection of information to predict risk and identify legitimate and rogue users of the networks. Application of the principle of collection limitation may be applied less rigorously in such instances. However, given the robust nature of the collection and the potential sensitivity of identifying information, an organization would be expected to implement security in a manner that addresses the risks raised by the collection, use and retention of that information.³

4. The Centre encourages organizations' use of privacy impact assessments as a tool to assess and manage risks that data use may pose to individuals. However, such assessments are not the appropriate tool to serve the transparency function suggested in the Department's framework.

Organizations have used privacy impact assessments to manage risks to individuals since as early as 1993. They are an essential tool for organizations as they put privacy protections into place and test new products, services and processes for risk to individuals. They are also key to an organization's decisions about implementing appropriate privacy protections. Many organizations conduct hundreds of privacy impact assessments every year.

In limited instances, privacy impact assessments can enhance transparency about an organization's data practices. For example, to address public concern about an emerging technology or business offering, it may be appropriate to make a privacy impact assessment available to the public for purposes of education or to enhance consumer trust. However, as a general rule privacy impact assessments carried out in the private sector are not intended to serve as a transparency device, and publication of the findings of a privacy impact assessment, as suggested in the Department's framework document, is not appropriate.⁴ In the vast majority of cases, privacy impact assessments are part of a broader *internal* assessment process and form part of the basis for decisions within the organization. An organization may conduct a privacy impact assessment and determine that a proposed application or business model raises risks to individuals that the organization cannot tolerate or mitigate appropriately, and consequently decide not to move forward. Or it may carry out an assessment, and based on its findings modify its new offering to reduce its customers' exposure to risk.

³ The application of analytics to large data sets in an effort to understand trends and predict future events represents another area where fair information practices should be applied in a manner that reflects the context of the data use. In his recent paper, "Data Protection Law and the Ethical Use of Analytics," Professor Paul Schwartz raises concerns about the appropriate application of principles of collection minimization and use limitation when an organization uses analytics to better understand what insights data might yield.

⁴ The Centre recognizes that privacy impact assessments have been used as a transparency tool in the public sector and recognizes their value when used in this way. However, such documents are often highly nuanced and carefully reviewed and revised prior to their publication, and their use by government does not argue for their use by private industry where considerations related to the data may differ markedly.

Privacy impact assessments may contain significant amounts of proprietary information, and its publication could reveal to competitors information about new products, services and offerings. Organizations might therefore be persuaded to oversimplify or sanitize privacy impact assessments or to generate versions of reports that avoid any liability or compromise to reputation. Furthermore, requiring organizations to make the results of all of their privacy impact assessments public might discourage organizations from carrying them out at all and deny industry the benefits of privacy impact assessments.

The Centre believes that privacy impact assessments should continue to serve as an important tool for responsible organizations that wish to base their data management decisions on a clear understanding of privacy risks their products, services and technologies raise. The Centre is concerned that, should they be made public as required by the Framework, organizations will limit their use and lose the advantage of the important insights they provide.

5. While the Centre encourages the establishment of a Privacy Policy Office in the Department of Commerce, it cautions that its charter should be clear and appropriate. Development of voluntary codes of industry conduct is best carried out by the organizations affected in a non-government environment that encourages candid and open negotiation.

The Centre has long encouraged establishment of a non-regulatory, Executive Branch office focused on consumer privacy. We suggest such an office could appropriately identify issues, conduct research, encourage common approaches to commercial privacy protection among government agencies, convene forums and meetings to explore contentious issues, encourage development and facilitate vetting of safe harbor programs, and stay abreast of how business processes and technologies are emerging and evolving over time.

The Centre is concerned that, as described in the proposed framework, the office would become inappropriately central to development of codes of conduct. While it is appropriate for such an office to motivate industry to develop those codes and encourage engagement of all stakeholders in the development process, the codes must be voluntary, and stakeholders will need a forum for frank, candid deliberation and negotiation that does not involve observation or comment by government and/or media. It will of course, be necessary for such an office to set goals, define the contours of such guidance, receive progress reports and vet the product. But the process must be run, and the pen held, by the interested stakeholders who will need to abide by the codes of conduct.

6. We recommend that the privacy office take a lead role in discussions in international organizations, and that the Federal Trade Commission continue to represent the United States in forums concerned with privacy regulation.

The Department of Commerce has played a key role in privacy policy development through its work at the OECD and the Asia Pacific Economic Cooperation, and in bilateral negotiations and trade discussions. It has served as an effective, trusted representative for US interests in that capacity, and we encourage the Department to continue in that role.

We commend the partnership that has emerged between the Department and the Federal Trade Commission as they fulfill their respective roles in privacy deliberations in international forums. The Federal Trade Commission's position as the point organization in forums oriented to regulatory issues and that require the participation of a regulatory authority -- such as the International Conference of Data Protection and Privacy Commissioners, the Article 29 Working Party, and other international privacy regulatory organizations -- remains important to the success of U.S. efforts.

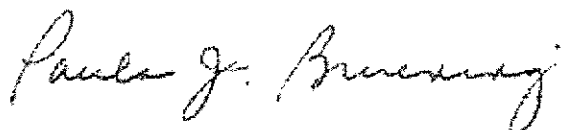
Conclusion

The Centre appreciates this opportunity to participate in the Department's work to address issues of commercial data privacy. We hope that the Department will look to the Centre as a resource, and are available to provide further information or to elaborate on the comments above. Please direct any questions to Martin Abrams at mabrams@hunton.com or Paula Bruening at pbruening@hunton.com.

Yours sincerely,



Martin E. Abrams
Executive Director



Paula J. Bruening
Deputy Executive Director

APPENDIX

UPDATING THE OECD GUIDELINES FOR THE 21ST CENTURY:
FIRST THOUGHTS

Fred H. Cate¹

The OECD 1980 Guidelines

Modern data protection law is built on “fair information practices.” According to Professor Paul Schwartz, a leading scholar of data protection law in the United States and Europe, “[f]air information practices are the building blocks of modern information privacy law.”² Marc Rotenberg, president of the Electronic Privacy Information Center, has written that “Fair Information Practices” have “played a significant role” not only in framing privacy laws in the United States, but in the development of privacy laws “around the world” and in the development of “important international guidelines for privacy protection.”³

One of the earliest and broadest efforts to identify the principles necessary to strike the delicate balance between privacy and the responsible use of information was led by the Organization for Economic Cooperation and Development (“OECD”). The OECD Committee of Ministers’ 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*⁴ (“Guidelines”) identified eight principles to “harmonise national privacy legislation and, while upholding such human rights, ...at the same time prevent interruptions in international flows of data.”⁵ They were designed to “represent a consensus on basic principles which can be built into existing national legislation” and to “serve as a basis for legislation in those countries which do not yet have it.”⁶ In this aspiration they have undoubtedly succeeded because most of the dozens of national and regional privacy regimes adopted after 1980 claim to reflect the OECD Guidelines.

The Guidelines’ eight principles are:

1. Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

¹ Distinguished Professor, C. Ben Dutton Professor of Law, Director of the Center for Applied Cybersecurity Research, Director of the Center for Law, Ethics, and Applied Research in Health Information, Indiana University; Senior Policy Advisor, the Centre for Information Policy Leadership at Hunton & Williams LLP. The author alone is responsible for the views expressed herein.

² Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” 52 *Vanderbilt Law Review* 1607, 1614 (1999). Professor Schwartz describes FIPPS as being “centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight.” *Id.*

³ Marc Rotenberg, “Fair Information Practices and the Architecture of Privacy: What Larry Doesn’t Get,” 2001 *Stanford Technology Law Review* 1 ¶ 43.

⁴ O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

⁵ *Id.* at preface.

⁶ *Id.*

3. Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
 - a. with the consent of the data subject; or
 - b. by the authority of law.
5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle—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.
8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.⁷

Under the OECD Guidelines, data processors have certain obligations without regard for the wishes of individual data subjects. For example, the data quality and security safeguards principles appear non-negotiable. Other obligations focus significantly on individual consent. For example, under the use limitation and purpose specification principles, the use of personal data is restricted to the purposes for which the data were collected, purposes “not incompatible with those purposes,” and other purposes to which the data subject consents or that are required by law. Still other principles—for example, the openness and individual participation principles—are designed entirely to facilitate individual knowledge and participation.

⁷ *Id.* ¶¶ 7-15.

New Challenges to Protecting Privacy

A great deal has changed since the OECD adopted its Guidelines in 1980. Advances in digital technologies have greatly expanded the volume of personal data created as individuals engage in everyday activities. “With the rise of new networks,” *BusinessWeek* wrote in its August 28, 2008, cover story, we are “channeling the details of our lives into vast databases. Every credit-card purchase, every cell-phone call, every click on the computer mouse [feeds] these digital troves. Those with the tools and skills to make sense of them [can] begin to decipher our movements, desires, diseases, and shopping habits—and predict our behavior.”⁸ The data routinely generated, collected, and stored include:

- What individuals buy and the other transactions in which they engage through 30 billion checks, 26 billion debit card transactions, 22 billion credit card transactions annually.
- What individuals communicate with family, friends, and colleagues in more than 30 billion emails a day. We send 173 billion text messages per month. These are all captured digitally, together with voicemail and Voice Over IP conversations, by someone other than, or in addition to, the sender.
- Location information. As of 2010, there are 5 billion mobile phones worldwide—almost double the figure just four years ago—which 95 percent of users say they keep within three feet of themselves at all times. Mobile phones thus constitute the world’s largest sensor network. Through GPS and triangulation, these phones generate increasingly precise information about the location, speed, and direction of movement of the user. Many cars contain navigational systems that include a GPS receiver. Laptops, PDAs, and cell phones that connect to WiFi necessarily provide information concerning the user’s location. Electronic toll payment systems provide a stream of location data to anyone with an appropriate reader.
- What individuals watch, listen to, and read through digital satellite and cable, iTunes, Amazon, and hundreds of other entertainment service providers and vendors.
- What individuals are doing in the office, in public, and increasingly even at home with video and audio surveillance, key-cards, security systems, keystroke monitoring, stored email and voicemail, and remote access to networked files. In 2006, 200 traffic surveillance cameras in London sent 8 terabytes of data a day to the central command center.
- What individuals are interested in, looking for, or concerned about. As of fall 2010, Internet users generated about 113 billion searches a month, doubling every two years, and visited an estimated 255 million websites, 15 times the number a decade earlier.
- Data on individuals and their families, friends, and co-workers through social networking, 152 million blogs, photo and video sharing, peer-to-peer file-sharing, virtual worlds, and even remote storage of documents and financial information—what is often called “cloud computing.” 5 billion photos were hosted on Flickr as of September 2010. 2 billion videos are watched on YouTube every day. Facebook alone has more than 518 million active users who

⁸ “Introduction to Book Excerpt: *The Numerati* by Stephen Baker,” *Businessweek*, Aug. 28, 2008. Ironically, the 2008 story is actually referring to a January 23, 2006, cover story, “Math Will Rock Your World.”

upload more than 20 million videos and spend more than 700 billion minutes on Facebook every month. 25 billion Tweets were posted on Twitter in 2010.

"Today, our biographies are etched in the ones and zeros we leave behind in daily digital transactions,"⁹ Stanford Law School Professor and former dean Kathleen Sullivan has written. Personal digital data increasingly describe and define our lives, and those data, according to Marc Rotenberg, are "recording [our] preferences, hopes, worries and fears."¹⁰

At the same time, demand for personal data from business, the government, and other organizations is escalating. Access to personal data facilitates increasingly targeted products, services, and advertising. It makes possible greater user convenience, efficiency, and recognition. Personal information is regarded as increasingly essential to security and accountability.

Moreover, technology has not only contributed to an explosion in the ubiquity of data, but also the range of parties with physical access to those data, and the practical and economic ability of those parties to collect, store, share, and use those digital footprints. For example, in a credit or debit card transaction, the data are collected by the retailer, the transaction processor, the card issuer, the cardholder's bank, and the merchant's bank. Digital networks have also facilitated the growth of vigorous outsourcing markets, so information provided to one company is increasingly likely to be processed by a separate institution. Records containing personal data are linked and shared more widely and stored far longer than ever before, often without the individual consumer's knowledge or consent.

George Washington University Law School Professor Daniel Solove writes: "We are becoming a society of records, and these records are not held by us, but by third parties."¹¹

Privacy Principles for the 21st Century

In the face of such dramatic changes since the OECD Guidelines were adopted 31 years ago, it is not surprising that they might require updating. While one is hesitant to tinker with principles that have undergirded all modern data protection laws, the focus of the Guidelines on discreet information exchanges seems outdated in a world of ubiquitous data flows. It is unclear whether individuals and data processors ever struck informed bargains over what data were being collected, for what purposes, and under what conditions, but that model appears so out of touch with today's reality as to require revision.

Fortunately, the careful wording of the Guidelines and the far-sightedness of their drafters allow for updating with minor, but important, revisions. These proposed changes serve the Guidelines' goal of protecting privacy without stifling innovation or expression and of "ensur[ing] that transborder flows of personal data . . . are uninterrupted and secure" and that data protection regimes are "simple and compatible."¹²

Here is one starting place:

⁹ Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 128, 131 (2003).

¹⁰ Louise Story, "To Aim Ads, Web is Keeping Closer Eye on What You Click," *New York Times*, Mar. 10, 2008, at A1.

¹¹ Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *75 Southern California Law Review* 1083, 1089 (2002).

¹² O.E.C.D., *supra* at ¶¶ 16, 20.

1. ~~Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Data should not be collected in a manner likely to cause unjustified harm to the individual unless required by law. “Harm” may include more than physical injury or financial loss. Harm is “unjustified” if caused by unfair or unlawful collection or use of data, or by processing in violation of the Data Quality Principle.~~
Collection Limitation Principle—Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Data should not be collected in a manner likely to cause unjustified harm to the individual unless required by law. “Harm” may include more than physical injury or financial loss. Harm is “unjustified” if caused by unfair or unlawful collection or use of data, or by processing in violation of the Data Quality Principle.
2. Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. ~~Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. Organizations should collect and store data only as necessary to serve lawful purposes, and should make information about those purposes readily available.~~
Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. Organizations should collect and store data only as necessary to serve lawful purposes, and should make information about those purposes readily available.
4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used:
 - a. for purposes likely to cause unjustified harm to the individual; or
 - b. over the well-founded objection of the individual, unless necessary to serve an over-riding public interest,~~unless required by law, other than those specified in accordance with [the Purpose Specification Principle] except:~~
unless required by law, other than those specified in accordance with [the Purpose Specification Principle] except:
 - a. ~~with the consent of the data subject; or~~
 - b. ~~by the authority of law.~~
5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle—An individual should have the right with regard to data concerning, or used in a manner affecting, employment, health care, financial matters, or legally protected rights:
 - 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.
- 8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above, and should be liable for the reasonably foreseeable harm caused by his failure to do so. Enforcement of data protection laws should achieve effective compliance with these principles and applicable law, while minimizing the burden on individuals or lawful information flows.

These changes are designed to serve specific goals that take into account the demonstrated success of the Guidelines, the significant changes in information technologies and applications over the past three decades, and the exceptional importance of privacy in an information age.

First, they respond to the reality that consent is an unworkable basis for most data processing activities and provides poor protection for privacy.¹³ Second, they seek to impose an obligation that the collection and use of data be fair, lawful, and unlikely to cause harm—irrespective of whether or not there is consent. Third, they recognize that harm is a broader concept than just physical injury or financial loss. Fourth, they acknowledge that harm may be justifiable (for example, if a criminal suspect is apprehended on the basis of accurate, lawfully obtained information). What makes a harm unjustifiable is if the data are not collected or used fairly and otherwise lawfully, if the data are inaccurate, or if they are linked to the wrong person.

Fifth, the proposed changes to the Guidelines recognize that a well-founded objection to a use of data may be sufficient to block the intended use, but that such an objection may be overcome by an overriding public interest. Sixth, the suggested language recognizes that the full range of individual participation rights should only apply where data concern, or are being used in a manner affecting, important matters or rights. Extending this principle to other data or other settings would in many cases be impossible given the way in which data are collected and stored, and could reasonably be anticipated to impose significant costs without yielding commensurate benefits. Finally, these changes seek to move beyond a mere compliance model to a broader understanding of accountability, in which organizations are stewards of the personal data that they collect, store, or use, and should be liable for the reasonably foreseeable harms that their failure to adhere to these principles causes.

The suggested changes otherwise leave the balance of the Guidelines unaltered. Security and transparency remain vital, along with the Guidelines' focus on flexibility, proportionality, and consistency across jurisdictions.

The language of the original Guidelines was carefully negotiated to address a variety of issues and cultural norms. Moreover, the Guidelines are supplemented by valuable commentary that provides additional details and guidance as to the drafters' intentions. The care with which the Guidelines and the commentary were drafted undoubtedly helps explain why the Guidelines have proved so influential and so durable. Any changes should certainly undergo similar scrutiny and discussion, and should be accompanied by appropriate commentary as well. The purpose here, therefore, is not to be overly focused on the actual wording of specific changes, but rather to indicate the types of changes necessary if the Guidelines are to retain their relevance in the 21st century.

¹³ See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, Dec. 2010, 19-21, 25-28, available at www.ftc.gov/os/2010/12/101201privacyreport.pdf.

**Centre for Information Policy Leadership
at Hunton & Williams LLP**

**Commentary in Response to the
European Commission's
Communication on
“A comprehensive approach to
personal data protection”**

January 2011

Executive Summary

Two Priorities

1. Accountability is an essential instrument for effective data protection and enforcement. It reinforces – but does not replace – legally binding ways for ensuring respect for the fundamental right to data protection. It encourages organisations to adopt and demonstrate tailor-made policies, procedures and practices for fulfilling the Data Protection Principles. It is not a self-regulatory tool, but does provide substantial scope for maximising effectiveness and minimising the burdens - the “Holy Grail” for data protection.
2. We propose a new framework of Binding Global Codes to improve and streamline arrangements for international transfers. This involves a re-cast BCR process, based on the Accountability Principle, where bespoke Codes with binding effect will be used to demonstrate and ensure practical compliance with the Data Protection Principles on a worldwide basis. We develop this proposal in more detail in a separate Paper.

More generally....

A modernised European framework for data protection is needed to address the realities of the digital world of the 21st Century.

The Centre agrees that EU Data Protection Principles remain sound, but argues that reform must focus on implementation and practicalities. The current approach is widely seen as not effective as it might be, with too many uncertainties and excessive burdens.

The Centre suggests criteria for a modernised regulatory framework, based on clear objectives, real risks and well-balanced outcomes.

We strongly support the Transparency principle, but stress its limitations. We have severe doubts about the efficacy of EU standard-form Privacy Information Notices which will be so comprehensive, or so simple, as to be meaningless either way. A sophisticated approach is needed, based on “reasonable and legitimate expectations”, with more attention on mis-statements.

There must be clarity of objective with data breach requirements, close attention to practicalities and avoidance of “breach fatigue”.

We support efforts to simplify rights of access, rectification, erasure and blocking, but are sceptical about a simple “Right to be Forgotten”. More

discussion is needed, probably focused on use restrictions.

Promoting the free flow of information is an important policy goal - globally as well as within the EU internal market. Harmonisation must be based on common principles and objectives, avoiding both highest and lowest common denominators. Harmonising regulatory approaches, including robust education programmes, is as important as the substance of the law itself.

Welcoming the commitment to reducing the administrative burden, we support attention on Notification requirements which do not serve any useful purpose. We support a very simple registration system designed to increase funding for DPAs and provide them with channels of communication for enforcement and education.

We welcome the emphasis on Privacy Impact Assessments and “Privacy by Design”, but a cautious approach is needed which encourages their use as business processes without crude mandatory requirements. We take the same approach towards Data Protection Officers.

1. Introduction

1.1 The Centre for Information Policy Leadership, associated with Hunton & Williams, encourages responsible information governance in today's digital society. Through collaboration with industry leaders, civil society and consumer organizations and government representatives, it explores innovative and pragmatic approaches to global policy issues, seeking to build privacy and data protection in practice while balancing economic and societal needs and interests. More details about the Centre can be found at www.informationpolicycentre.com.

1.2 The Commission and many other commentators are already aware of the work on Accountability which the Centre has supported through the Galway and Paris projects. The two main Discussion Documents are “*The Essential Elements of Accountability*”¹ and “*Demonstrating and Measuring Accountability*”².

1.3 The Centre welcomes the European Commission’s Communication on “*A comprehensive approach to personal data protection*” which is an important milestone on the route towards improving the data protection framework at EU level. We especially welcome the Commission’s recognition that the challenges of technology and globalisation are now driving the need for reform with unprecedented urgency.

¹ http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

² http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

1.4 This Commentary is deliberately selective – not attempting to address every issue raised by the Commission, but instead focussing on key points which we would be happy to elaborate through meetings or correspondence. Drawing on the Centre's activities and experiences in recent years, our **top priorities** are to build the case for a new regime for:

accountability as an essential instrument for effective data protection and enforcement; and

international data transfers, undertaken in accordance with the Accountability principle, which will achieve good standards of data protection on a world-wide basis.

The structure of this Commentary broadly follows that of the Communication itself, with a separate Paper setting out more detail on the proposed new approach to international transfers.

2. Principle and Pragmatism

2.1 Although some may argue that an entirely fresh start should be made with the regulatory framework, the Centre understands and generally endorses the approach adopted by the Commission. There is broad agreement across the EU institutions, and across wider informed opinion, that the Data Protection Principles “remain sound” and that the “highest priority” should be given to “ensuring respect for the fundamental right to data protection”. This reflects the much-increased public, political and commercial interest in privacy and data protection world-wide. Beneath some different language, there is in fact a surprising amount of common ground across the issues raised in the Communication and reforms now under active discussion in the USA, notably in response to thinking within the Federal Trade Commission and the Department of Commerce and at Congressional level. The Centre has provided considerable thought leadership into these debates and has deep insights into them. We would be happy to share this experience with the Commission if that would be helpful.

2.2 It is important that the reform agenda prioritises implementation and practicalities. Despite endorsement of the Principles, the current EU approach is widely seen as not effective as it might be, not least because of too many uncertainties and excessive bureaucracy and burden which can deter good practice. Only recently has it become widely seen that processing personal data properly involves much more than formal rights and duties and legal compliance. Good information governance is cultural and must also embrace corporate and employee behaviours, training and awareness programmes and acceptable deployment of technology. There has been a transformation since the Directive was adopted in 1995, with the majority of commercial organisations now driven by reputational, financial and other reasons for **wanting** to process personal data properly.

2.3 It is also welcome that the Commission in effect recognises that data protection now impacts on virtually every organisation of whatever size or sector. With such a range of business types and business model, and such widespread use of technology, it is important to recognise that “One size cannot fit all” and to avoid approaches which are excessively prescriptive. Even the smallest organisation can now process vast amount of sensitive personal data. The digital age - with powerful devices, instant wireless, mobile and fixed communications, open networks, more effective search and analytical tools and ever-cheaper data storage capacity - creates seemingly endless opportunities to gather and interpret information about us, our activities and our preferences. Data about anyone can be easily copied and aggregated around the world across vast, interconnected networks.

2.4 The criteria for a modernised, 21st Century, regulatory framework for Europe are that the legislation should:

- be based on clear objectives which are focussed on real threats to fundamental rights and the risks of other personal or social harm;
- aim for outcomes which reflect social norms;
- ensure a good balance between the benefits and the harms of processing personal data;
- promote good practice, while imposing minimum standards;
- be cast in accessible and relevant language which will facilitate predictable and consistent results;
- avoid stifling innovation by being technologically neutral and future-proof; and
- be internationally compatible, or at least inter-operable.

2.5 A specific reform consistent with our overall approach and these criteria would be to exclude business contact information (names, office addresses, e-mail and telephone details) from the definition of personal data. This exclusion across the EU – as already explicitly provided in Spain – would immediately and significantly reduce the burden of compliance with little real cost to personal privacy.

2.6 It has been widely recognised that the Centre has provided and stimulated detailed thinking which shows how the Accountability Principle meets these aspirations with a flexible and effective tool to promote high standards. This can be secured through legislation with a focus on clear objectives and outcomes, with requirements and incentives to identify and address both general and specific risks in each case. This also helps DPAs to move increasingly to from *ex ante* to *ex post* approaches, making a reality of the “Selective to be Effective” mantra and prioritising their attention on the poor performers who ignore the fundamental right to data protection or do not take it seriously.

2.7 To summarise, the underlying goal for new legislation should be to pursue the “Holy Grail” for data protection of:

- maximising effectiveness (in terms of both protection and free flows of information); and
- minimising burdens.

3. Strengthening individuals' rights

Transparency

3.1 The Centre has always been a strong supporter of the Transparency principle and welcomes the Commission's commitment to it. It must be right that individuals should be as well-informed as possible about the processing of their personal data. We agree that this must involve the use of accessible and plain language, whether online or offline. This is important in both private and public sectors. In the former, information for consumers is an important driver and enabler of competition and promotes privacy as a competitive element. In the public sector, readily understandable information about the existence, nature and extent of the processing is vital to the State/Citizen relationship.

3.2 However, the goal for transparency must not be to place the burden for compliance on individuals. It is important to be aware of the limitations of Transparency. First, there is now ample evidence the "Notice and Consent" model of data protection regulation, which places a great burden on individuals to read and understand privacy notices, is not especially effective in practice, as shown by the overwhelming empirical evidence that individuals do not read – let alone respond to - Privacy Notices, especially if they are lengthy. The Centre's 2004 project on Layered Notices emphasised the need to ensure that individuals do not receive more information than they want or can digest. But, even with a Layered approach, the default position is likely to remain that even the simplest notices will not be read.

3.3 Second, we have severe doubts about the efficacy of EU standard-form "Privacy Information Notices". There are so many data controllers and processors, with such diverse goods and services, with so many different business models marketing to consumers with so many different characteristics and needs that – even if they could be drafted - any standard form notices will inevitably be so comprehensive, or so simple, as to be meaningless either way. One size cannot fit all. The Centre's 2007 White Paper, *"Ten steps to develop a multi-layered privacy notice"*³, undertaken in cooperation with the OECD, demonstrates the real difficulties of drafting Notices, even for specific situations.

3.4 These limitations do not make transparency irrelevant, but they do point to the need for a sophisticated approach. For example:

- There is no need for explicit disclosure of "obvious" information;

³ (http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf)

- The legislative priority should be on disclosure – preferably on a “just in time” basis - of any processing which goes *beyond* the “reasonable and legitimate expectations” of the individual;
- Consent should not be necessary except in unusual, novel or otherwise sensitive situations;
- In line with the Accountability principle (see below) the regulatory priority should be action against mis-statements - essentially Notices which are false or misleading when matched against reality;
- Data protection should learn and borrow from other areas of EU consumer protection (e.g. food labelling) and develop a “traffic light” regime to give people immediate reassurance or warning (and drive standards higher.)

3.5 Consideration could also be given to a “Use and Obligations” framework for implementation and interpretation of the EU Data Protection Principles in a manner that reflects and serves the way data is used and managed in the 21st century. This approach switches focus onto the way an organization **uses** data to determine its **obligations** towards data subjects and to determine the appropriateness of the data and its processing. Obligations include such matters as transparency (notice), choice, access and correction. The model also focuses on the internal steps an organization should take to minimise risk to both the organization and the individual — covering such matters as data minimisation (collection and use); data quality and integrity; data retention and security. More details were set out in the 2009 discussion document on “*The use and obligations approach to protecting privacy*”⁴.

4. Breach Notification

4.1 The Centre recognises the powerful pressures for a mandatory breach notification regime. In other jurisdictions, the experience has been very diverse - regimes can be effective, burdensome or ineffective. Much depends upon clarity of objective (e.g. deterrent, punitive or compensatory?) and how the practicalities are addressed. It is especially important to avoid “breach fatigue” and to address a range of key issues. What types of personal data should be covered or excluded? Which types of breach should be notified? How best to avoid expensive notifications where the harm is minimal? Who should be notified – regulators or individuals? How much detail? With what consequences? These and other issues are explored more fully in two publications from the Centre:

- *Do's and don'ts of data breach and information security policy*⁵; and
- *Information Security Breaches - Looking Back & Thinking Ahead*⁶

⁴ http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf

⁵ http://www.huntonfiles.com/files/webupload/CIPL_Dos_and_Donts_White_Paper.pdf

⁶ http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf

5. Rights of access, rectification, erasure and blocking and the “Right to be forgotten”

5.1 The Centre is supportive of efforts to simplify rights of access, rectification, erasure and blocking and to make them more effective in practice.

5.2 However, we are both unclear and sceptical about the so-called “Right to be forgotten”. If this means more than the existing rights of erasure and blocking it would come close to “re-writing history” - i.e. bringing about changes to records about factual events. A widely-drafted provision extending to complete deletion of material which may be embarrassing or damaging could have dangerous cultural, political and human consequences and is anyway likely to be opposed by all those who support freedom of speech and press.

5.3 This is not to dismiss the idea of a Right to be Forgotten altogether. We recognise considerable interest and discussion around the subject which may have utility in some circumstances and with respect to some kinds of data. Deeper thinking and reflection are clearly required here. One promising avenue may be to introduce more limited restrictions and limitations which focus on the use, rather than the retention, of types of data. For example it may be acceptable to restrict the use of retained police records to police purposes, banning for example their release for vetting purposes. Other examples – though not easy to achieve in practice - would be a right to demand deletions from a social network site or a presumption against access by employers to such sites. In any event, any right to oblivion should not extend beyond personal data which is readily accessible in the ordinary course of business.

6. Enhancing the internal market

6.1 As data flows ever more freely, this is an important dimension – globally as well as within EU. Further harmonisation is very important and very welcome in principle as divergence between national laws is very burdensome.

6.2 But harmonisation, both within and beyond Europe, must not aim for highest or lowest common denominators, but rather on common principles and objectives. This is especially important if there is to be any meaningful regulatory control as more and more organisations embrace cloud computing and other activities beyond conventional geographical and jurisdictional boundaries. Harmonization would not be welcome if it were based on stringent procedural requirements that would impose significantly greater burdens in some Member States and/or exclude major trading partners in Asia and North America.

6.3 The Centre certainly agrees that higher priority should go on harmonising regulatory approaches in practice than on substantive laws. As well as ensuring that DPAs are adequately staffed and resourced, the new legislation

should impose a duty upon them to develop and execute robust privacy education programmes aimed at controllers, processors and individuals.

7. Reducing the Administrative Burden

7.1 The Centre very much welcomes the Commission's commitment to reducing the administrative burden. As mentioned, the "Holy Grail" for data protection should be maximising effectiveness in practice whilst minimising unnecessary burdens.

7.2 We especially support the wish to revise and simplify the Notification requirements. These are seen as ineffective and expensive, particularly for companies needing to provide and update a mass of detailed information in different ways in up to 27 countries. Radical re-thinking is required as to whether Notification currently serves any useful purpose. The concept was originally designed in a different era when it may have made sense for the regulators be provided with details of relatively few processing activities, mainly on a small number of mainframe computers.

7.3 We welcome the suggestion of a new registration system. Our vision – whether registration is at pan-EU or Member State level - is that nothing more is needed from data controllers than basic details of corporate identity and a reasonable registration fee which could be kept by the DPA. This approach provides increased funding (which is unlikely to come from public funds for the foreseeable future) **and** enforcement and educational channels of communication for DPAs. This would reinforce the Commission's calls for better resources and for more efforts at awareness-raising.

7.4 As the Article 29 Working Party has effectively recognised, the Accountability Principle – elaborated below – makes it easier to switch from Notification to Registration. It is more effective, more efficient and less burdensome to hold data controllers themselves accountable for complying with data protection requirements in practice than to impose a bureaucratic requirement to notify details of processing in advance and expect over-burdened DPAs to spot any problems. It may be necessary to reinforce a Registration system with powers (to the extent that they are lacking) for the DPA to demand details of processing from a data controller and to inspect processing in particular cases. This approach would be another desirable step towards "*ex post*" enforcement and would bolster new emphasis on targeted enforcement.

8. Enhancing Data Controllers' Responsibility / Accountability

8.1 The Centre welcomes the emphasis in the Commission's Communication on policies and mechanisms for ensuring compliance. As pointed out above, getting data protection right involves much more than legal compliance with formal rights and duties. Good information governance is cultural and must embrace both the awareness and behaviours of data controllers and their management and staff and how they use technology.

8.2 We especially welcome the reference to the Accountability Principle in this context, but this needs to be further developed. The papers emerging from the Galway and Paris projects have already been mentioned and contain much material suggesting approaches (especially in relation to international transfers) which would be both effective and widely welcomed. The Article 29 Working Party's *Opinion 3/2010 on Accountability* is a further valuable contribution⁷. One very important point to make here is that the Accountability Principle is **not** a matter of self-regulation. It reinforces – but does not replace – legally binding ways for ensuring respect for the fundamental right to data protection. But its flexibility and encouragement for tailor-made policies and procedures to fulfil the Data Protection Principles also reflect that responsible companies want or need to process personal data properly. A statutory requirement for putting the essential elements of accountability into effect, as recommended by the Article 29 Working Party, would expand the number of responsible organizations and facilitate more effective enforcement.

8.3 The essential elements of Accountability can be summarised as:

- organisational commitment to **bespoke** internal policies which elaborate the general Principles
- mechanisms to develop and put policies into effect, including procedures, technologies, training and education
- systems for ongoing internal oversight, assurance reviews and external verification
- focus on risks and outcomes
- transparency
- readiness to **demonstrate** the chosen approach to compliance.

8.4 Although the greatest and most sophisticated opportunity to put the Accountability Principle into legislative effect arises in the context of international transfers (see below), a more general obligation on all data controllers to demonstrate their approach to compliance can also be envisaged. But this must be seen – as did the Article 29 Group - as a means of **reducing** the administrative burden, not just a matter of “aiming not to increase the burden”. In this respect we felt that the Commission's Communication is distinctly unambitious. The scope to abandon Notification requirements is one example where the burden can be reduced; another is the potential for more flexible sanctions where companies can demonstrate their compliance efforts.

9. Privacy Impact Assessments / “Privacy by Design”

9.1 Our support for the Accountability Principle means that we also welcome the Communication's emphasis on Privacy Impact Assessments and the use of “Privacy by Design”. These are both elements of an accountability programme, which encourages organisations to identify and manage risks and to take a holistic approach to the deployment of technology.

⁷ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

9.2 The risks arising from processing personal information include:

- threats to fundamental rights and freedoms
- harm to individuals – economic, social, autonomy/dignity
- harm to organisations – reputational, financial, operational
- harm to society – relationships, trust, social stability.

9.3 Privacy Impact Assessments have rapidly become seen as the optimum way of identifying and addressing privacy risks by reference to their seriousness and likelihood. We support the use of PIAs by accountable organizations to discover and mitigate risk. However, there is a global discussion about using PIAs as a transparency device and a cautious approach is necessary. PIAs should be encouraged selectively, and with incentives, and not imposed universally. If companies were required to make all PIAs public, their effectiveness as a internal risk management device would be reduced.

9.4 We also welcome in principle the support for the “Privacy by Design” concept as a business process. In 2009 the Centre co-authored *“Privacy by Design: Essential for Organizational Accountability and Strong Business Practices”*⁸, which the Commission may find helpful. We believe that the concept should be actively encouraged, but again it is hard to envisage how it could be universally imposed. We recognise, however, that much will depend upon the precise legislative drafting and will respond to any specific proposals in due course.

9.5 The Centre is supportive of the role of Data Protection Officer. If there is to be corporate accountability, it follows that there need to be personal accountabilities and responsibilities inside the organisation. We have reservations, however, about the possibility that (as in Germany) the role should be made mandatory for organisations above a certain threshold. The main risk is that the appointment of a DPO becomes formulaic, resulting in appointees who (though notionally independent) lack real power and influence. It is striking that Chief Privacy Officers who have been appointed on a voluntary basis tend to operate at a much more senior level and have achieved strong strategic influence⁹. An obligation to appoint a DPO with standard-form functions could easily become an intrusive burden with no real benefit.

10. Encouraging Self-Regulatory Initiatives and Certification Schemes

⁸ http://www.hunton.com/files/tbl_s47Details/FileUpload265/2911/Privacy_by_Design_Abrams.pdf

⁹ If desired, the Centre could arrange for the Commission to receive copies of the IAPP’s 2010 Surveys of Role, Function and Salary for both European Data Protection Professionals and Global Privacy Leaders.

10.1 Codes of Practice are superficially welcome, but a cautious approach is needed. In fact, there is a spectrum of different types of “self-regulation”. “Pure” self-regulation, with no reference to the legal framework, is not binding and brings risks of ineffectiveness, anti-competitiveness and/or unfair advantage to companies who choose not to self-regulate. At the other extreme, there is nothing distinctive or valuable about so-called self-regulation which is externally imposed and scarcely differs from legal requirements.

10.2 We prefer the approach of “Co-Regulation”, where there is a clear and binding legal framework of principle which both requires and encourages companies to decide and demonstrate how they achieve the desired outcomes in their own way. At domestic and international level, this is one of the main attractions of the Accountability Principle – minimum imposed burden and maximum effectiveness in practice.

10.3 The Centre is pleased that the Commission will be exploring the feasibility of Certification schemes. Validation and certification issues formed a central part of the Paris phase of Accountability project and Commission may find it helpful to refer to the resulting report on Demonstrating and Measuring Accountability¹⁰. The key issues include: What is being certified? By whom? With what authority? and How meaningful will the “certificate” be for consumers? There are risks of high cost, limited practicality and threats to innovation which again point towards encouragement and incentive rather than compulsion. Drawing upon both successful and problematic schemes around the world, the Centre would be pleased to discuss the opportunities and the limitations of Certification schemes with the Commission.

11. The Global Dimension

11.1 We have already made clear that our top priority is to build the case for a new regime for international data transfers, undertaken in accordance with the Accountability principle, which will achieve good standards of data protection on a world-wide basis.

11.2 Articles 25 and 26 of the existing Directive have been simultaneously its most controversial and most burdensome provisions. It is also arguable that they have been the least effective if full account is taken of current volumes of international transfers. The wish to protect EU citizens on a worldwide basis when their personal data is transferred is understandable and not in doubt. We are sceptical about the value or practicality of “clarifying” the Adequacy procedure and there are well-rehearsed problems or limitations with standard contract terms and the Safe Harbor arrangement. The result is the paradox that substantial resources are expended by some organisations trying to “get it right” whilst there is unmeasured non-compliance by other organisations which ignore the requirements.

¹⁰

http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

11.3 We therefore wholeheartedly welcome the commitment to “improve and streamline” arrangements for international transfers. We see this as by far the most pressing priority for reform and are aware that other studies have reached the same conclusion. We consider that the most promising way forward is to build on the Binding Corporate Rule (BCR) approach. Reform is needed which will:

- establish a clear legal foundation for a BCR-type process;
- ensure that high standards of data protection are achieved globally in practice;
- be truly scalable to meet the needs of an integrated global economy which already has 63,000 recognisable multi-national companies and millions more SMEs which are regularly transferring personal data internationally;
- not place unrealistic demands upon over-stretched and under-resourced DPAs

11.4 We consider that “**Binding Global Codes**” (BGCs) are the best way forward. This approach is a re-cast BCR process based on the Accountability Principle, but scalable and without the current (but inevitable) delays and bureaucracy associated with BCRs. The BGC proposal allows and incentivises an organisation to develop and implement its own bespoke Code with a set of binding rules for demonstrating and ensuring compliance with the Data Protection Principles on a worldwide basis. The Code must meet minimum requirements and must be publicised and the organisation must be held accountable for fulfilling its terms. This means that DPAs would be empowered to investigate and impose meaningful sanctions in any case where either the Code itself does not impose sufficiently rigorous standards in line with the Data Protection Principles or the organisation has failed to meet the requirements of its own Code. This is consistent with the emphasis which we place on action against false or misleading privacy statements.

11.5 A separate Paper which we are submitting simultaneously to the Commission sets out our analysis and concrete proposals in more detail, with specific legislative proposals.

The views expressed in this paper are those of the Centre for Information Policy Leadership. They do not necessarily reflect the views of the Centre’s members or those of Hunton & Williams LLP or its clients.

**Centre for Information Policy Leadership
at Hunton & Williams LLP**

**A New Approach to International
Transfers**

**In Response to the European
Commission's Communication on
"A comprehensive approach to
personal data protection"**

January 2011

Executive Summary

Reforming the regime for international transfers is by far the most pressing priority for reform of the EU Data Protection Directive. There is a paradox that substantial resources are expended by some organisations trying to “get it right” (if only in legal paperwork) whilst there is unmeasured non-compliance by other organisations which ignore the requirements. This discredits the EU legislation and does little to secure genuine data protection when personal data leaves Europe.

We believe that a new framework for international data transfers, built on the experience with BCRs and explicitly grounded on the Accountability principle, could be achieved with “**Binding Global Codes**” (BGCs). This approach addresses the scale of the challenge with millions of transfers occurring daily, but without the current (but inevitable) delays and bureaucracy associated with BCRs.

The BGC proposal allows an organisation to develop and implement its own bespoke Code with a set of binding rules for demonstrating and ensuring compliance with the Data Protection Principles and their practical implementation on a worldwide basis. The Code must be publicised and the organisation must be held accountable for fulfilling its terms. This means that DPAs would be empowered to investigate and impose meaningful sanctions in any case where either the Code itself does not impose sufficiently rigorous standards or the organisation has failed to meet the requirements of its own Code.

This paper concludes with a first draft of legislation to illustrate the approach that we have in mind for inclusion within a new Directive or Regulation.

1. Introduction

1.1 The Centre for Information Policy Leadership, associated with Hunton & Williams, encourages responsible information governance in today's digital society. Through collaboration with industry leaders, civil society and consumer organizations and government representatives, it explores innovative and pragmatic approaches to global policy issues, seeking to build privacy and data protection in practice while balancing economic and societal needs and interests. More details about the Centre can be found at www.informationpolicycentre.com.

1.2 This Paper is complementary to the Centre's main Commentary responding to the European Commission's Communication on “A comprehensive approach to personal data protection”. The purpose of this separate and self-contained Paper is to set out in more detail our proposals for a new approach to international data transfers. We are proposing a new legislative framework for transfers undertaken in accordance with the

Accountability principle, which will achieve good standards of data protection in accordance with the EU Data Protection Principles on a world-wide basis. We would be delighted to discuss our proposals at a further level of detail through meetings or correspondence with the Commission.

1.3 The Centre welcomes the Commission's recognition that the challenges of technology and globalisation are now driving the need for reform with unprecedented urgency. We see the issue of international transfers as by far the most pressing priority for reform. Articles 25 and 26 of the existing Directive have been simultaneously its most controversial and most burdensome provisions. It is also arguable that they have been the least effective if full account is taken of current volumes of international transfers. The wish to protect EU citizens on a worldwide basis when their personal data is transferred is understandable and not in doubt.

1.4 We therefore wholeheartedly welcome the commitment to "improve and streamline" arrangements for international transfers. But we are disappointed that the Commission's thinking appears to be still incomplete and that concrete suggestions have not yet been put forward. Moreover, we are sceptical about the value or practicality of "clarifying" the Adequacy procedure and there are well-rehearsed problems or limitations with standard contract terms and the Safe Harbor arrangement. At the moment is the paradox that substantial resources are expended by some organisations trying to "get it right" (if only in legal paperwork) whilst there is unmeasured non-compliance by other organisations which ignore the requirements. This discredits the EU legislation and does little to secure genuine data protection when personal data leaves Europe.

2. Binding Corporate Rules – Successes and Limitations.

2.1 The optimum international framework for international data transfers needs to recognise that good data protection cannot arise from laws, rules, policies and procedures alone. It is now also a matter of corporate and information governance, needing:

- top leadership and managerial commitment;
- IT enhancements and safeguards;
- employee awareness, training and supervision;
- cultural reinforcement; and
- incentive and deterrent pressures driven largely by considerations of organisational reputation.

2.2 The Binding Corporate Rules (BCR) approach – originally documented by the Article 29 Working Party in 2003 and developed in further Opinions since then - has been a welcome attempt in principle to address these challenges. It is widely seen as a brave attempt to improve the protection of fundamental rights in the international context. European DPAs deserve recognition and credit for developing and exploring BCRs as a way to address these challenges.

2.3 The BCR approach has *in principle* been attractive to businesses and regulators and has generated positive responses. Businesses especially value the scope for tailoring their own BCR within a template of minimum requirements to address their own circumstances. This approach recognises that good practice for data protection - applying general principles to particular circumstances – is inevitably context-specific. This approach is a good example of modern co-regulation. It is also an excellent example of the Accountability Principle which the Centre has supported through the Galway and Paris projects. The two main Discussion Documents are “*The Essential Elements of Accountability*”¹ and “*Demonstrating and Measuring Accountability*”².

2.4 However the **problems** associated with BCRs – principally delay and expense – are now **very serious**. Although the pace has quickened in the last two years, very few BCRs have actually been delivered. (It is thought that fewer than 20 BCRs have so far been approved or are near to approval.) Delays occur both in negotiations with the lead DPA and in securing clearance from the other 26 DPAs across the EU, even where the Mutual Recognition agreement applies. The causes of delay arise from novelty, unfamiliarity, complexity (legal, cultural, corporate) and the wide differences from one type of multinational organisation to another.

2.5 Above all, however, the problem is lack of resources within DPAs. BCRs are concentrated within a few lead authorities, and those authorities are limited in their ability to expand resources.

2.6 Moreover, the relentless expansion of the digital society means that the authorities must place greater priority on effective enforcement against (or guidance for) those organizations which deliberately, ignorantly or cavalierly make little or no effort to protect personal data. It will be increasingly untenable for DPAs to devote growing attention to the **lower** priority of BCR negotiations (where broadly well-intentioned businesses are trying to get it right).

2.7 A 2003 Yale study conservatively estimated that there are some 63,000 multinational corporations, with 821,000 subsidiaries. They directly employ 90 million people and produce 25 per cent of the world's gross product. It can be asserted with confidence that that every single multinational corporation now transfers personal data internationally. Beyond that, there are countless SMEs and other organisations which are not “multinationals”, but which are nevertheless involved daily in international transfers of personal data, often of a highly sensitive nature. In short, it is inconceivable that the BCR approach – without improvement - could meet the potential underlying demand.

2.8 In summary, the BCR approach is therefore now facing:

the risks of failure – businesses will give up or not apply; and / or

¹ http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

² http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

the risks of success – even if more BCRs are approved, DPAs will become totally swamped and delays will get much worse and paralyse the entire system.

This situation will seriously **damage the credibility** of BCRs, of European DPAs and of all attempts to regulate international data transfers.

A new approach – modernisation building on conceptual success with BCRs – is now needed with some urgency. New features (substantive and process) must aim at (1) improving the attractions to businesses (who will wish to minimise the burden) and (2) improving the value to regulators (who will wish to increase their effectiveness in securing maximum levels of compliance and good practice). A new approach must realistically migrate from the test-bed of very low volumes to mass-production.

3. Accountability in Practice

3.1 The Galway and Paris Projects have put Accountability firmly on the agenda, both generally and within the context of reform of EU data protection law.

3.2 The essential elements of Accountability can be summarised as:

- organisational commitment to **bespoke** internal policies which elaborate the general Principles
- mechanisms to develop and put policies into effect, including procedures, technologies, training and education
- systems for ongoing internal oversight, assurance reviews and external verification
- focus on risks and outcomes
- transparency
- readiness to **demonstrate** the chosen approach to compliance.

3.3 Accountability reinforces – but does not replace – legally binding ways for ensuring respect for the fundamental right to data protection. But its flexibility and encouragement for tailor-made policies and procedures to fulfil the Data Protection Principles also reflect that responsible companies want or need to process personal data properly. A statutory requirement for putting the essential elements of accountability into effect, as recommended by the Article 29 Working Party, would expand the number of responsible organizations and facilitate more effective enforcement.

*“..it would be appropriate to introduce in the comprehensive framework an accountability principle...[This] would require data controllers to have the necessary internal mechanisms in place to **demonstrate compliance** to external stakeholders, including national DPAs.....”*

“The new provision could be included....even in the case the data have been

transferred to other controllers outside the EU.”

*Article 29 WP / WP on Police & Justice
The Future of Privacy, Dec 2009*

“Data protection must move from theory to practice. Legal requirements must be translated into real data protection measures”

“One size does not fit all”

“[Accountability offers ways to] implement appropriate and effective measures to put into effect the Directive’s Data Protection Principles and obligations”

*Article 29 WP Opinion on Accountability
July 2010*

3.4 Although this is not explicit, accountability has in fact always been the foundation of the BCR approach. In effect, adherence to a set of Binding Corporate Rules signifies that a business is prepared to demonstrate its commitment to compliance and good practice and can be held accountable (by regulators and stakeholders) for fulfilment of that commitment.

*The [BCR] rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The issuing by the headquarters of internal privacy policies must be regarded only as a first step in the process of adducing sufficient safeguards within the meaning of Article 26 (2) of the Directive. The applicant corporate group **must also be able to demonstrate** that such a policy is known, understood and effectively applied throughout the group....”*

*Article 29 WP
WP 74, Binding Corporate Rules, 2003*

4. Binding Global Codes

4.1 We are proposing a new approach - **Binding Global Codes (BGCs)** – based on the following propositions:

- The BGC Framework would be built on an explicit foundation of Accountability.
- A multinational organisation which adopts and implements an acceptable Binding Global Code would accept responsibility for its fulfilment and for ensuring delivery of fundamental rights. In return – and for so long as that remains true - it would be treated as satisfying EU and other requirements for international data transfers.

- A Binding Global Code would take the form of a set of binding rules demonstrating compliance with the Data Protection Principles on a worldwide basis and meeting certain other minimum requirements.
- The Code must cover policies, procedures, technology and human/organisational issues – not just legal compliance - with clear governance arrangements and identifiable internal responsibility.
- The governance arrangements should extend to mandatory internal assurance or verification arrangements
- The Code must apply globally to all processing by the organisation of personal data (unless explicitly excluded) and (by contract) to all those with whom the data is shared.
- The code must be formally adopted by the organisation through a defined standard procedure.
- The Code must be publicised and the organisation must be held accountable for fulfilling its terms. Publicity could be mandated through website notices, media announcements, annual reports, filing with regulators and listing bodies etc.
- Organisations would self-certify their own Code without the need for prior DPA approval, which is simply not practicable with the scale of the challenge.
- DPAs would be empowered to investigate and impose meaningful sanctions in any case where either the Code itself does not impose sufficiently rigorous standards in line with the Data Protection Principles or the organisation has failed to meet the requirements of its own Code. This is consistent with the emphasis which we place elsewhere on action against false or misleading privacy statements.
- If self-certification is considered too radical, there are other options for the initial adoption or approval of a Binding Global Code to ensure that the minimum requirements are in fact met. These include certification by an independent Third Party (“Accountability Agent”) appointed by the DPA at the expense of the business or certification by a Third Party approved by the DPA.
- There is a corresponding need for meaningful sanctions – injunctive, punitive and remedial - where an organisation fails to fulfil its own Code. Accountability means facing the consequences of failure, including failure to fulfil publicly-adopted commitments.
- With scope to re-direct resources more effectively, a new priority for regulators – collaborating internationally – must be to enforce compliance in practice. The emphasis would be on holding

organisations to account for the commitments they have assumed by adopting their Code. Effective regulatory interventions must be expected where:

- o the content of a Binding Global Code in fact fell below the requirements;
 - o inspection or audit reveals non-compliance with commitments given in the Code;
 - o complaints or incidents reveal such non-compliance;
 - o self-declaration – e.g. where the organisation is required to notify the regulatory or listing authority of specific or systemic non-compliance.
- Individuals would be entitled to pursue claims against an organisation where liability arises because they are denied the rights guaranteed to them under its Code.
- To the extent that mandatory requirements of local law are inconsistent with the BGC approach, such requirements would need revision, probably at EU level.
- The BGC approach has the potential to align with equivalent provisions in the APEC Privacy Framework to achieve a genuinely global solution, but perhaps with the robust substance which would flow from European leadership.

4.2 To summarise, a Binding Global Code would be the vehicle for the organisation to handle international flows of personal data in ways which are lawful, which ensure standards of good practice respecting the integrity of the data and which bring internal discipline to the business. Organisations striving to handle personal data well, in compliance with legal requirements and good practice, would have a major incentive for adopting a Code – provided they can avoid the burden and delay of advance negotiation and prior approval.

5. Suggested Legislation

5.1 We will be happy to participate in further discussions to develop the BGC approach further. At this stage, the following text, based otherwise on the provisions of the existing Directive, is a first draft to illustrate the approach that we have in mind:

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, a data controller (or member of its corporate group [as defined]) may transfer personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) on condition that:

- a. the transfer takes place in accordance with a Binding Global Code adopted by that data controller; and
 - b. the data is processed, and continues after transfer to be processed, in accordance with that Code.
2. A “Binding Global Code” means a set of legally binding rules which require contractually or otherwise, that regardless of location:
 - a. the personal data will be processed in accordance with the principles and obligations set out in the Directive; and
 - b. adequate safeguards will be observed with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.
3. “Legally binding” means that:
 - a. the rules are legally enforceable and binding in practice so that the controller is liable, whether to a supervisory authority or to any adversely affected data subject, for any non-compliance with them; and
 - b. the controller is committed to demonstrate to a supervisory authority on request how compliance is and will be achieved.
4. A Binding Global Code shall also contain other measures, including those of a technical or organisational nature, directed at promoting compliance with the principles and obligations set out in the Directive and with good practice in the processing of personal data.

The views expressed in this paper are those of the Centre for Information Policy Leadership. They do not necessarily reflect the views of the Centre's members or those of Hunton & Williams LLP or its clients.

Data Tagging for New Information Governance Models

The ubiquitous collection, use, and flow of data challenge existing frameworks for data protection and management. Organizations collect and derive data from myriad sources and use it for a wide variety of purposes, so that the rules that apply

to their data holdings vary. A company might use data for internal processes such as product development and accounting in one instance, and in another transfer that same data for processing by a vendor or business partner half-way around the world.

Although geography and national borders place few inherent limitations on where organizations can transfer data, such boundaries demarcate different and very real requirements and obligations for handling personal information. For owners and processors, moving data across these boundaries presents practical challenges in administering and implementing the rules and laws by which individuals maintain their rights to data protection and privacy.

Here, we describe data governance in this complex and dynamic environment, where the rules and obligations that govern how organizations use and protect information attach to the data and must be met wherever or by whomever it is collected, processed, or stored. We can facilitate such an approach via “tagging” data with sufficient information that its recipients and users can understand their specific obligations for its appropriate use and safeguarding.

Emerging Approaches to Data Governance

The emergence of nearly instantaneous collection, analysis, use, and sharing of data has prompted policymakers, privacy experts, businesses, and regulators to call for new approaches to securing and governing it. Various forums have highlighted current governance models’ limitations. In its December 2009 “Opinion on the Future of Privacy,” the Article 29 Data Protection Working Party expressed the view that the present legal framework hasn’t been fully successful in ensuring that data protection requirements translate into effective mechanisms that deliver real privacy protection.¹ Its 13 July 2010 release proposes a legal system architecture that would integrate an accountability approach to data protection.² Organizations participating in the US Federal Trade Commission’s (FTC’s) “Exploring Privacy” workshop series emphasized cur-

PAULA J. BRUENING
Centre for Information Policy Leadership, Hunton & Williams LLP

K. KRASNOW
WATERMAN
Massachusetts Institute of Technology

less procedure-based privacy protection that includes “substantive restrictions on data privacy processing designed to prevent specific harms.”³ The Center for Democracy & Technology, in contrast, argues for grounding privacy protection in a more comprehensive iteration of fair information practices that incorporates principles beyond notice and choice.⁴)

New models proposed for information protection and privacy reflect and respond to the realities of 21st century data collection, analytics, use, and storage. These approaches realistically take into account where notice is effective and where individual choice and control are appropriate and real. They reflect information’s role as a critical business asset and the challenge of responsibly managing data within organizations. Such models include accountability;⁵ the application of fair information practices based on data use, rather than its collection;⁶ and a comprehensive system of securing and managing data referred to as *strategic information management*.⁷

These approaches recognize that if data protection and management are to be effective, the obligations to protect and secure data attach to the data itself and must be met wherever it’s stored or processed. They also rely on the ability to tag data with information about those obligations, so that all relevant parties can understand and meet them. Such obligations might arise from law and regulation, self-regulatory guidelines and best practices, and the promises organizations make to individuals about how they will protect and responsibly use those individuals’ data. For example, when the fictional online retailer BuyWeb collects data from customers to fill an order, deliver goods, facilitate internal processes such as billing and accounting, and provide customer service, this data collection might be governed by

one or more laws, self-regulatory guidelines, and privacy promises. BuyWeb is committed to fulfilling those governance obligations. When it makes data available to an outside vendor—for instance, to process billing or respond to customer inquiries—the requirement to meet those obligations doesn’t end; the vendor must also follow the applicable rules.

Imagine that a BuyWeb customer moves from Tokyo to Los Angeles or London. BuyWeb notes the move and enters the address change into its customer database. The address change means that the individual’s home jurisdiction and the laws that apply to his or her data have also changed. BuyWeb must first determine whether the new or old jurisdiction’s rules apply to previously collected data and then both apply the correct rules in its own systems and ensure that its business or process partners do the same.

Organizations have also begun to appreciate data’s full value as a critical business asset and to take a comprehensive approach to protecting it. Companies understand that they should safeguard and manage data in ways that not only protect individuals’ privacy but also ensure data’s integrity and availability for a wide range of uses within the company. BuyWeb will want to use the customer’s change in address to accurately market weather- or culture-related products. Different co-branding or supply-chain partners will likewise wish to capitalize on the updated information.

Data must also be available when called for in judicial and legal proceedings, an increasingly complex problem as jurisdictions have developed apparently contradictory requirements.^{8,9} For example, a customer service representative might appropriately look at a customer’s address to verify a caller’s identity or determine if a shipping address matches company records.

That same representative might be precluded from seeing credit-card information if not taking an order. New approaches to data protection within companies involve setting rules about data access, use, storage, and retention, and ensuring that employees follow those rules as data flows throughout the organization.

To facilitate these new approaches to data protection and management, data protection obligations must *attach to and travel with the data*. Individuals must be able to rely on the law, best practices, and the company’s representations about its data practices, no matter who processes that data, or when. Users and data custodians must understand and follow the rules that govern who may use data within the organization, in what ways, under what circumstances, and to further what ends. Third-party data processors must be able to understand what requirements they must meet and the specifications about how they may use data. These approaches would guarantee that individuals receive protection in a decentralized, networked data environment, where they might have no knowledge of, and little choice about, the actual party or parties handling their information.

Accountability

An accountability principle has been a feature in both the earliest major international instrument on privacy—the Organization for Economic Cooperation and Development’s Privacy Guidelines¹⁰—and the most recent—the Asia Pacific Economic Cooperation (APEC) Privacy Framework.¹¹ Both require that the information owner or data controller “should be accountable for complying with measures that give effect” to the fair information practices articulated in the guidelines.^{10,11}

Efforts are currently under way to define the contours of accountability and explore the conditions

that an organization must demonstrate and that regulators must measure to certify accountability. Policymakers, regulators, and experts have described an accountable organization as one that sets privacy protection goals for companies based on external criteria established in law, self-regulation, and best practices, and vests the organization with the ability and responsibility to determine appropriate, effective measures to reach those goals. Given that the complexity of data collection practices, business models, vendor relationships, and technological applications in many cases outstrips individuals' ability to make decisions through active choice about how their data is used and shared, accountability requires that organizations make disciplined decisions about data use even absent traditional consent.

Accountability's essential elements are organizational commitment to accountability and adoption of internal policies consistent with external criteria; mechanisms to put privacy policies into effect, including tools, training, and education; systems for internal, ongoing oversight and assurance reviews and external verification; transparency and mechanisms for individual participation; and means for remediation and external enforcement.

As an accountable organization, BuyWeb might establish an internal privacy and data management policy consistent with both local laws and regulations and the promises about privacy it makes to consumers. Under an accountability approach, BuyWeb would also implement mechanisms to ensure that employees adhere to those policies and systems for internal risk assessment and mitigation, including oversight and assurance reviews. Those systems would govern how the organization handles information internally. BuyWeb might also use an outside vendor located in

Vietnam to provide customer service and address complaints about products or billing. In this case, the rules that govern the data apply even when the outside vendor is doing the processing. BuyWeb will have to ensure that the vendor is committed to and capable of meeting these obligations.

In another example, BuyWeb might wish to avoid addressing cross-jurisdictional legal requirements as much as possible and might thus create an internal policy to limit the receipt of customer data outside each individual's home jurisdiction. It might implement this policy in part through mechanisms that look for clues (IP address or telephone area code) about where an incoming customer request is coming from and route it to a service representative in the same jurisdiction. The organization would later provide validated reporting about its performance, perhaps including the numbers or percentage of employees trained on the policy in the prior year, or of requests successfully routed according to the policy.

Central to an accountability approach is the organization's ongoing assessment and mitigation of the risks inherent to individuals from information use. In the case of the routing-service-requests-to-matching-jurisdiction example, the retailer would also capture and analyze the incidents that didn't comply with the policy and attempt to identify modifications to the practice or technology to improve future performance.

Use-and-Obligations Model

The use-and-obligation model establishes data use rather than its collection as primarily driving users' obligations to protect and safeguard information. Collecting data and consumer consent to or choice about its use traditionally have triggered an organization's obligations. In this model,

however, the mere fact that an organization collects information from a customer wouldn't typically trigger an obligation. Instead, this would occur only, for example, if the company used the customer's address to confirm his or her identity or direct a package delivery. The use-and-obligations model proposes a framework for implementing and interpreting traditional principles of fair information practices that addresses how companies can use and manage information in the 21st century. It incorporates the full complement of fair information practices, including transparency and notice, choice, access and correction, collection limitation, data use minimization, data quality and integrity, data retention, security, and accountability.

The use-and-obligations model takes into account all uses that might be necessary to fulfill the consumer's expectations and meet legal requirements. It imposes obligations on organizations based on five categories of data use:

1. fulfillment activities necessary to establish and maintain the relationship between the organization and consumer;
2. internal business operations and processes necessary to operate a business, such as accounting, product development, and personnel management;
3. marketing;
4. fraud prevention and authentication; and
5. national security and legal requirements imposed by courts and government.

In our BuyWeb example, checking a customer address to confirm identity would fall under use number 4 and to direct a package would fall under use number 1. The obligations based on these uses that apply to the data must be met even if the data is shared or processed by a third party.

Strategic Information Management

Strategic information management is an integrated approach to managing data across an enterprise to minimize risk and enhance competitive opportunities.¹² It envisions not simply protecting personally identifiable information but all information assets. It recognizes that information is a critical business resource and appropriately protects and manages data in a way that facilitates the organization's compliance with legal requirements and minimizes the risk using that information might raise to the company and its customers. Managing information strategically requires that companies make decisions about data that ensure that it's available to the appropriate personnel when needed, and fosters new and creative use that can add value for the organization and consumers.

For example, an organization might decide that to protect its data resources, it will adopt a policy-based access control system, a method that restricts access to data based on predetermined rules. Under this broad umbrella might be rules about handling information that are designed to protect trade secrets, others implementing privacy law, and still others ensuring that the organization meets fiduciary responsibilities. For instance, BuyWeb's competitiveness might be based on a cheaper cost of goods than its competitors; its company policy might treat the sources of goods as a trade secret and protect that high-value data by limiting access to its suppliers' identities to those people who negotiate acquisition terms or receive the goods at the port of entry. BuyWeb's implementation of OECD guidelines might prohibit access to individual customer data to anyone in the accounting department, except individuals directly addressing customer complaints and corrections. And, perhaps,

BuyWeb has decided to centralize fulfilling its statutory obligations to file sales tax payments in all the countries where it operates, allowing only assigned workers in the corporate tax office and auditors access to the tax calculation and payment data. These access rules serve a different purpose but share a common structure: people with a particular responsibility are permitted to access particular data for a particular purpose.

Practical Considerations

Each of these new models relies on individuals' and organizations' responsibility to handle data—whether at rest, in transition, or in motion, and whether in a centralized or decentralized environment—in accordance with rules. These rules about handling information fundamentally share a common structure—they describe a policy (such as, permit, require, or prohibit) about whether an entity (a person, organization, or system) may use particular data (data type, subject, provenance, and so on) in a particular way (collect, copy, merge, share, delete, and so on) under certain circumstances. Consider some policies we've described:

- The entity called customer service is permitted to use data about a customer's address to verify identity.
- The company's computer systems are required to route customer service requests to customer service representatives in the same jurisdiction.
- The company is prohibited from addressing a package to an address not in the customer's profile.

Data custodians' ability to ensure that their organization follows all necessary rules depends entirely on their ability to identify the data, the actor, the transaction, the circumstances, and some means to associate those factors with the rules

that govern them. Although we can perform such identification manually, the volume of data and transactions has made human review an impractical approach to the challenges; computer-assisted review is now required. Systems can recognize such data (about actors on the data, about the data itself, or about the actions and circumstances) if it's annotated, or tagged.

Computer systems aren't human clones. They can't consistently glean meaning from whole sentences nor independently implement complex logic. Even so, privacy rules can be incrementally implemented in digital environments by reducing the text to something that looks more like an algebra problem:

- IF (Entity called "Customer Service") AND (Data category "Customer's Address") AND (Purpose of Use is "Verify Identity"), THEN Permitted.
- IF (Data category "Shipping Address") NOT SAMEAS (Data category "Customer's Address"), THEN Prohibited.

This is how programmers write instructions that computers can understand. They identify categories of information that are relevant to the business activity (such as "entity," "data category," and "purpose of use"). Depending on the rule, the programmer might pre-define the only things that can be placed in that category or permit other people or systems to put anything in that category. If the data in a system is tagged to identify such categories, then a computer can gather the necessary information to implement policies.

If all information necessary for implementing a privacy rule existed in a single database, then tagging might not be so important. To understand why, consider a corollary from the pre-digital world: a business might have kept a customer's records in a file folder tabbed with the customer's name. Inside

a customer's file, the company might place a name, address, and account number, but the file typically wouldn't include the name or job duties of everyone who ever opened the file, put something in, or took something out. Nor would it include a list of questions the business had used the file to answer. But, even the simple rules we just described require information about the data in the database and data outside it—who's trying to use the information and why.

Typically, laws and contracts are even more complex. They have conditions and exceptions that might in turn have conditions and exceptions. They require knowledge about information sources, the date and time of acquisition, the proposed information recipients, the rules that applied to the data before the data holder received it, and many other facts not ordinarily collected in either the old-fashioned paper file folder or a typical digital data file. As entities tag these other sorts of data—data about provenance, transactions, associated rules, and so on—organizations can implement increasingly complex, automated or semi-automated rules processing. They can automate rules regulating acceptable information use, appropriate data protections, and transparency and accountability, and they can increasingly validate how consistently rules are applied, even after the data changes hands, purposes, or forms.

New approaches to governance attempt to respond to the new information environment, where data collection can occur in circumstances where traditional notice and choice might not be possible, sharing and analysis might happen in real time, and processing might take place outside the jurisdiction where information was collected. Data tagging offers a practical way to digitally attach obligations to in-

formation and reap the benefits of these new protection models. Legacy data systems raise important cost issues for organizations contemplating data tagging. While a growing market of products reduce those costs, policymakers and organizations will need to strike the appropriate cost-benefit balance as they consider this important path forward toward data protection that will serve the 21st century digital environment. □

References

1. "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*, Article 29 Data Protection Working Party, 2009; http://ec.europa.eu/justice_home/fsj/privacy/docs/spdocs/2009/wp168_en.pdf.
2. "Opinion 3/2010 on the Principle of Accountability," Article 29 Data Protection Working Party, 2010; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.
3. F.H. Cate, "The Failure of Fair Information Practice Principles," *Consumer Protection in the Age of the Information Economy*, J.K. Winn, ed., Ashgate Publishing, 2006.
4. "Refocusing the FTC's Role in Privacy Protection," *Comments of the Center for Democracy & Technology in Regards to the FTC Consumer Privacy Roundtable*, 6 Nov. 2009.
5. "Data Protection Accountability: The Essential Elements, a Document for Discussion," *The Galway Accountability Project*, Oct. 2009; www.ftc.gov/os/comments/privacyproundtable/544506-00059.pdf.
6. "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," *The Business Forum for Consumer Privacy*, 7 Dec. 2009.
7. P. Bruening et al., "Strategic Information Management," *Privacy & Security Law*, Bureau of Nat'l Affairs, vol. 7, no. 36, 2008.
8. *In re Advocat "Christopher X,"* Cour de Cassation, no. 07-83228, 12 Dec. 2007.
9. *United States v. Vetco*, *Federal Reporter*, 2nd Series, vol. 691, 1981, p. 1281 (US 9th Circuit Court of Appeals).
10. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 1980; www.oecd.org/document/18/0,2340,en_2649_34255_1815_186_1_1_1_1,00.html.
11. "APEC Privacy Framework," 2005; [www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~APEC+Privacy+Framework.pdf/\\$file/APEC+Privacy+Framework.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf).
12. "Strategic Information Management," *Privacy & Security Law*, Bureau of Nat'l Affairs, Sept. 2008.

Paula J. Bruening is Deputy Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP in Washington, DC. Her work focuses on cross-border data flows, emerging technologies, privacy accountability, and cybersecurity issues. Bruening has a JD from Case Western Reserve University School of Law. She recently spoke at the US Federal Trade Commission's "Exploring Privacy" workshop. Contact her at pbruening@hunton.com.

K. Krasnow Waterman is a visiting fellow at the Massachusetts Institute of Technology's Decentralized Information Group, prototyping accountable systems and launching a course on creating linked-data ventures. She's both a technologist and lawyer, has been a systems manager at JP Morgan, the inception CIO of a large federal counterterrorism task force, in private practice with Brown & Bain, and a Special Assistant US Attorney. Waterman has a JD from Cardozo School of Law. Contact her at kkw@mit.edu.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

THE CENTRE

FOR INFORMATION
POLICY LEADERSHIP

HUNTON & WILLIAMS

www.informationpolicycentre.com

© 2011 The Centre for Information Policy Leadership LLP. The content of this paper is strictly the view of the Centre for Information Policy Leadership and does not represent the opinion of either its individual members or Hunton & Williams LLP. The Centre does not provide legal advice. These materials have been prepared for informational purposes only and are not legal advice, nor is this information intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Please do not send us confidential information. Visit us at www.informationpolicycentre.com.