

June 14, 2010

National Telecommunications and Information Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams:

The Centre for Information Leadership (“the Centre”) appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration’s Notice of Inquiry, “Information Privacy and Innovation in the Internet Economy.” The Centre commends the Department for conducting this inquiry and for the important work it has undertaken to address this critical issue.

The Centre’s mission is development of sound 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 developing economies, and government use of private-sector data. The Centre has worked extensively with Asia Pacific Economic Cooperation (“APEC”) and the Organization for Economic Cooperation and Development (“OECD”) on issues of privacy and data protection. The Centre currently serves as secretariat for an international group of experts representing privacy protection agencies, civil society, academia and business that is exploring an accountability model for privacy governance.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. The Centre is located within the law firm of Hunton & Williams and is financially supported by approximately 40 companies. The Centre’s views and the views expressed in this response are its own and do not necessarily reflect those of its member companies, the law firm of Hunton & Williams LLP, or the firm’s clients. However, the organizations listed at the end of this submission have expressed their support for the Centre’s recommendations contained herein.

In its response to this inquiry, the Centre offers ten recommendations and attaches supporting documents.

Centre Recommendations

1. The Department of Commerce should represent the United States in global privacy discussions.

The Department of Commerce must play a lead role in representing US interests in international discussions on privacy and global data flows. Over the past decade the US the Department of Homeland Security and the Federal Trade Commission have served in that capacity. Both agencies have their appropriate role, and the Federal Trade Commission has been recognized as best qualified for accreditation to participate in international conferences of data privacy commissioners. However, the Department of Commerce is best positioned to develop and advocate for US policy that fosters economic growth; robust, innovative use of data; and protection of privacy in forums where issues related to privacy are cross-cutting with issues related to trade, outsourcing, innovation, and technology policy. The Department of Commerce has played this role effectively in the past, for example in its work at the OECD and on the EU-US Safe Harbor, and continues to do so at APEC. We urge the Department to lead engagement in other international multilateral forums and in bilateral negotiations.

The Department of Commerce should seek out our trading partners' knowledgeable, effective representatives to ensure that the appropriate privacy and data protection models are considered. It must continue conversations with data protection authorities, but also broaden those discussions to include experts in trade, industry and specialized fields such as pharmaceutical research, to ensure that policies reflect sound, creative thinking about innovation, the importance of robust global flows of data to trade and economic growth, and respect for privacy.

2. The Department of Commerce should continue to support development of policy frameworks that will support the global flow of data.

The Department of Commerce must continue to promote global policy frameworks that ensure the robust, accountable flow of data. The Centre believes that the Department's experience in negotiating the Safe Harbor with the European Commission and in its role in developing the APEC Privacy Framework should be brought to bear to eventually

create a global framework that facilitates the flexible, accountable flow of data. These frameworks work best when based on agreed-upon, common objectives for data protection. The Department of Commerce should lead stakeholders in a process to develop those common objectives.

3. The government should articulate a vision for innovation and privacy in the information economy.

The Department of Commerce must articulate a unified vision for an innovative, safe digital environment that serves an information-driven economy. Such a vision must reflect both benefits derived from the business innovation that is driven by data, including personal data, and the responsible protection and management of information. Privacy must be positioned within that overall vision, and innovative uses of information must be compatible with data practices that promote privacy.

4. Information policy must have a home within the government.

The executive branch must demonstrate ongoing support for this vision by establishing a non-regulatory office that coordinates information policy in the United States. The information policy office must be led and staffed by experts who understand the technology, economic interests and societal values at issue as new business models and data applications evolve. Its role should include reporting on the advantages and costs to innovation of privacy protection. This office could be situated within the Department of Commerce. While the Centre does not believe this office should have a regulatory role, the agency should coordinate with the regulatory bodies charged with oversight and enforcing private-sector laws on privacy, information security and cyber security. The agency should also coordinate with the Privacy and Civil Liberties Oversight Board, which has similar responsibilities related to the government's use of information.

5. Both industry and government must be accountable for its use of information.

To be innovative, organizations must be able to explore data to understand its predictive value. Today, almost all business processes begin with the question "what does the data tell us?" To encourage growth through innovative information use, industry must be empowered to explore and use data robustly and responsibly.

The flexibility to be innovative must be conditioned on the organization's accountability for the manner in which it uses, manages and protects data. Every use of information

affects privacy. To strike the appropriate balance between the value created by data use and the risk that use poses to privacy, organizations must implement privacy processes that are as dynamic as their business processes. To be successful, the innovative organization must understand the privacy risks to individuals associated with the innovative use, and stand ready to mitigate those risks.

The assumption of the responsibility for the risks associated with innovative data use, and the willingness to be responsible for those risks form the basis of an accountability approach to data protection.

The Centre, through its Galway Accountability Project, defined the five essential elements of accountability:

1. Organization 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 mechanism for individual participation.
5. Means for remediation and external enforcement.¹

Accountable organizations are responsible and answerable for the decisions they make about the use, management and protection of data. Accountability requires organizations to understand the risks they create for individuals by collecting and using information, and to mitigate those risks. In an environment where meaningful notice and choice become increasingly difficult to provide and exercise, accountable organizations make careful, balanced decisions about data, whether or not the individual has had an opportunity to make a choice about the use of his or her data. Accountability places the onus on organizations to be responsible about data, and relieves the individual of the burden of policing the marketplace against bad actors and

¹ The essential elements of accountability are more fully discussed in "Data Protection Accountability: The Essential Elements," October 2009, attached as Appendix A and found at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf> (last visited June 2, 2010).

making choices about data that may, in the end, provide little consumer control or protection.²

In recent months, accountability has figured prominently in discussions about how to improve privacy and data protection.³ Companies and policymakers are exploring how an accountability model for data protection might work in practice. What this inquiry has made clear is that accountability can only be effective for the private sector if government builds accountability into its information processes as well. The risk assessment and mitigation that lie at the heart of an accountability model must be adopted by government. While calls for such reform will likely be met with resistance, the private sector cannot be fully accountable if the federal government is not held similar requirements about the use and protection of data.⁴

6. Federal privacy law must pre-empt state laws.

U.S. business has repeatedly asserted that the “patchwork” of different, and often conflicting, state privacy laws impose significant burdens on companies that rely on data and data processing to run their business and power their product and service offerings. While many state legislatures have adopted innovative, effective approaches to privacy and security legislation, the nature of data use and data flows requires consistent, clear privacy law. Any federal privacy law should pre-empt state privacy laws from imposing requirements over and above those in federal legislation.

² The Safeguards Rule of the Gramm-Leach-Bliley Act provides an example of accountability that has worked well: the rule requires that companies secure their data, but leave decisions about how best to do so to the organization.

³ Discussion 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. At the Asia Pacific Economic Cooperation forum, models for implementation of the APEC Privacy Framework depend upon accountability to facilitate protected cross-border data flows. “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” notes the significance and utility of the accountability principle. 02356/09/EN WP 168, December 1, 2009, published January 11, 2010, by the Article 29 Working Party. Attached as Appendix B and available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf (last visited June 2, 2010).

⁴ A complete discussion of accountability can be found in “Data Protection Accountability: The Essential Elements; A Document for Discussion,” Attached as Appendix A and available at <http://www.ftc.gov/os/comments/privacyproundtable/544506-00059.pdf> (last visited May 27, 2010).

7. U.S. privacy policy should focus on successful privacy results rather than on procedures that do little to enhance privacy.

The US should avoid placing procedural requirements before strategic management of information and privacy protection. A checklist approach to privacy often results in a completed checklist rather than enhance privacy. Furthermore, the resources required to comply with procedural requirements often reduce those available to manage the real privacy risks to individuals. Some jurisdictions, for example, require companies to register all databases and notify officials if the data is to be processed in a manner different from that asserted, creating significant work for lawyers but providing little protection for individuals. In the U.S., advocates, experts and businesses have repeatedly commented that the annual privacy notices required by the Gramm-Leach-Bliley Act (but reportedly read by few consumers) have done little to promote privacy. In both cases, resources invested in complying with legal requirements would be better spent on initiatives that yield appreciable privacy results.

Alternative, comprehensive approaches to data management require that considerations and requirements for privacy, information security, and cyber security (as well as protection of intellectual property, trade secrets and evidentiary data) be part of an organization's overall data collection, storage, use and retention strategy. Governance approaches such as privacy by design, combined with accountability offer more effective information policy governance.⁵

8. Preventing harm must remain a significant feature of the U.S. approach to privacy.

Prevention of harm has been a feature of US privacy law since the enactment of the Fair Credit Reporting Act. Prevention of harm is a fundamental principle of the APEC Privacy Framework that supports setting priorities about data protection and enforcement based on the extent to which data practices may expose individuals to potential harm. The harm-based approach to privacy protection has come under criticism as focusing exclusively on financial and physical harm. But the potential for harm extends beyond the physical and financial to include the negative social impact harm to reputation, for example — that can result from the misuse of data. All three kinds of harm – physical, financial and social – should form the basis for setting protection and enforcement

⁵ Cavoukian, A., Abrams, M. and Taylor, S., "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," Office of the Information Privacy Commissioner, Ontario, November 2009, attached as Appendix C, and found at http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf (last visited June 2, 2010).

priorities. It will be important to carefully define the contours of social harm to provide businesses with a clear sense of their responsibility and the limits of their liability for such harm.⁶

9. The Department of Commerce should undertake an initiative to develop privacy norms that apply to data analytics.

Data analytics drive market innovation but also raise risks to individual privacy. Current data privacy guidance does not anticipate the power and speed of data analytics. The Centre urges the Department of Commerce to lead a process to set norms for analytics that encourage innovation, but create baseline guidance about their use in a manner that respects individual privacy. In developing those norms, it will be necessary to bear in mind the distinct differences in attitudes toward analytics that exist between the United States and its trading partners. Moreover, it will be important to recognize that no bright line has been identified between what information about an individual's behavior is and is not private.

Information and the ability to subject data to intensive analysis are essential to innovation and economic growth. With the freedom to understand the data comes the responsibility to use information in a judicious, disciplined fashion.

10. Privacy oversight and enforcement are best carried out by regulatory agencies with authority over specified industry sectors.

Any approach to privacy governance should preserve the current system whereby privacy is overseen by an industry sector's existing regulatory agency. Under such a model privacy enforcement benefits from the agency's intimate understanding of the challenges and opportunities companies face, the new business models and technologies companies adopt, the ways in which data is used and raises risks to privacy, and the overarching regulatory structure that governs the industry and that may impact the effectiveness of regulation or guidance and the opportunity for innovation and growth. Maintaining this system would preserve the value derived from familiarity with the way privacy governance works within an industry sector and within individual companies. In keeping with this model, the Federal Trade Commission should continue to oversee consumer privacy protection in general. As noted in Recommendation 3 of this submission, the Centre does not recommend creation of a

⁶ While notions of physical and financial harm are well established, the concept of social harm requires further exploration and definition. Such an inquiry is beyond the scope of this submission.

single privacy regulator, however it does believe there is a role for an office that would coordinate privacy, information security and privacy security policy in the private sector. That office would work with regulatory bodies to ensure that new technologies and business processes are reviewed and understood, and that policy guidance is applied consistently and appropriately across all sectors.

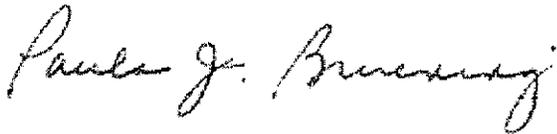
CONCLUSION

The Centre appreciates this opportunity to participate in the Department of Commerce's work to encourage data-driven innovation and effective privacy protection for individuals. 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 recommendation 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

The following lists organizations that support the above recommendations submitted by the Centre for Information Policy Leadership.

Acxiom

Experian

Google

Hewlett-Packard Company

IBM

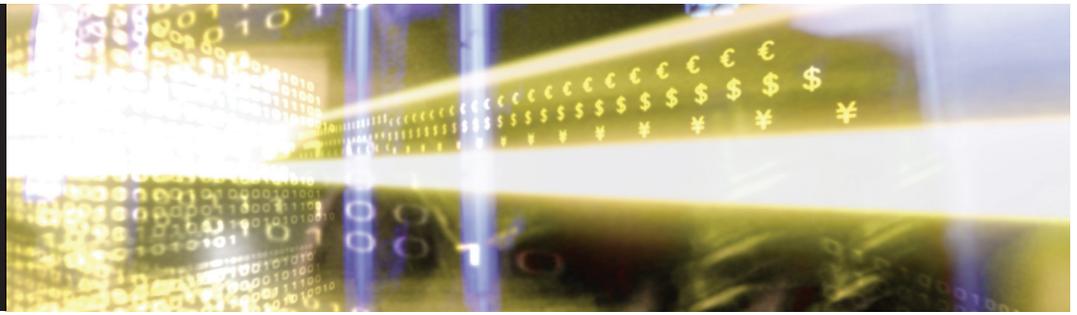
Intel

Microsoft

Oracle

salesforce.com

APPENDIX A



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.

APPENDIX B

ARTICLE 29 Data Protection Working Party

Working Party on Police and Justice



02356/09/EN
WP 168

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**

Adopted on 01 December 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

The Working Party on Police and Justice was set up as a working group of the Conference of the European Data Protection Authorities. It is mandated to monitor and examine the developments in the area of police and law enforcement to face the growing challenges for the protection of individuals with regard to the processing of their personal data.

Executive Summary

On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

The central message of this contribution is that the main principles of data protection are still valid despite the new technologies and globalisation. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency).
- Innovate the framework by introducing additional principles (such as ‘privacy by design’ and ‘accountability’).
- Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
- Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

Chapter 1 contains an introduction, with a brief overview of the history and context of data protection in the EU.

Chapter 2 proposes the introduction of one comprehensive legal framework. It recognises the need for specific rules (*leges speciales*), provided that they fit within the notion of a comprehensive framework and comply with the main principles. The main safeguards and principles of data protection should apply to data processing in all sectors.

Chapter 3 and 4 discuss the main challenges to data protection.

Chapter 3 on globalisation states that under EU law, data protection is a fundamental right. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. Individuals should be able to claim protection, also if their data are processed outside the EU. Therefore, the Commission is called upon to take initiatives towards the further development of international global standards regarding the protection of personal data. In addition, it is necessary to redesign the adequacy process. Furthermore, international agreements can be appropriate instruments for the protection of personal data in a global context, and the future legal framework could mention the conditions for agreements with third countries. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs). A provision on BCRs should be further reinforced and included in the new legal framework. Regarding applicable law, the WP29 envisages to advise the Commission on this subject in the course of the upcoming year.

Chapter 4 on the technological changes states that Directive 95/46/EC has stood well the influx of technological developments because of its sound and technologically neutral principles and concepts. These principles and concepts remain equally relevant, valid and applicable in today's networked world. The technological developments have strengthened the risks for individuals' privacy and data protection and to counterbalance these risks, the principle of 'Privacy by Design' should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies. The application of such principle would emphasize the need to implement privacy enhancing technologies, 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. This principle of 'Privacy by Design' should therefore not only be binding for data controllers, but also for technology designers and producers. On top of that, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

Chapters 5, 6 and 7 argue that these main challenges to data protection require a stronger role for the different actors.

The changes in the behaviour and role of the data subject, and the experience with Directive 95/46/EC, require a stronger position for the data subject in the data protection framework. Chapter 5 contains suggestions for empowering the data subject, in order to play a more active role. Empowerment of the data subject requires, among others, the improvement of redress mechanisms: more options for the data subject to execute and enforce his rights, including the introduction of class action procedures, more easily accessible, and more effective and affordable complaints procedures and alternative dispute resolutions. In addition, the new framework should provide alternative solutions in order to enhance transparency and the introduction of a general privacy breach notification. 'Consent' is an important ground for processing which could under certain circumstances empower the data subject. However, at the moment, it is often falsely claimed to be the applicable ground, since the conditions for consent are not fully met. Therefore the new framework should specify the requirements of 'consent'. Furthermore, harmonisation needs to be improved, as the empowerment of the data subject is currently being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Finally, the role of data subjects on the internet is an area of concern and should be further clarified in view of the new legal framework. In any case, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller.

Chapter 6 aims at strengthening the responsibility of the data controllers. Data protection should first of all be embedded in organizations. It should become part of the shared values and practices of an organization, and responsibilities for it should be expressly assigned. This will also assist national Data Protection Authorities (DPAs) in their supervision and enforcement tasks and therefore strengthen the effectiveness of privacy protections. Data controllers need to take several proactive and reactive measures, mentioned in this chapter. Furthermore, it would be appropriate to introduce in the comprehensive framework an accountability principle, so data controllers are required to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data, and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including DPAs. Notifications of data processing operations with national

DPA's could be simplified or diminished. It should be explored whether and to what extent notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases, and how notification could be streamlined.

Chapter 7a envisages stronger and clearer roles for national DPAs. At the moment, there are large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs. The new challenges to data protection require strong supervision by DPAs, in a more uniform and effective way. The new framework should therefore guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.

Chapter 7b states how the cooperation of the DPAs should be improved. The European DPAs are united in the WP29. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. In addition, the working methods of the WP29 should be further improved. Where needed, it should be insisted on that there is a strong commitment of members of the WP29 to implement the views of the WP29 into national practice. Relations between the WP29 and the Commission, that provides for the Secretariat of the WP29, can be further improved by describing the main roles of both players in a Memorandum of Understanding. The WP29 will enter into consultation with the Commission regarding this Memorandum in 2010.

Finally, Chapter 8 discusses the data protection challenges in the field of police and law enforcement, an area of specific concern. The context of this area within the EU has changed with the entry into force of the Lisbon Treaty. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters can be seen as a first step towards a general framework in the former third pillar, but is far from complete. Over the last years, there has been a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector, due to growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime, and stimulated by the technological developments. Against this background, the challenges for data protection are immense, and should be addressed in the future legal framework. Chapter 8 provides the conditions for law and policy making on data protection in the area of police and law enforcement: basing information exchange on a consistent strategy; a periodic evaluation of existing measures, legal instruments and their application; transparency, and addressing access and rectification rights in a cross border context; transparency and democratic control in the legislative process; the architecture of systems for storage and exchange of personal data; a clear framework as a basis for relations with third states, that is binding on all parties and based on the notion of adequacy; special attention for large scale information systems within the EU; properly addressing independent supervision, judicial oversight and remedies; and strengthening cooperation between DPAs.

1. Introduction

The consultation

1. On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges.
2. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

History and context

3. The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)¹ can be considered as the first European legal framework for the fundamental right to protection of personal data. The right to data protection is closely related but not identical to the right to private life under Article 8 of the European Convention for Human Rights. The right to data protection is recognised as an autonomous fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union.
4. The principles of Convention 108 were refined in Directive 95/46/EC² which forms the main building block of data protection law within the EU. The (future) effectiveness of the directive is the main object of the consultation of the Commission. Other EU legislative instruments for data protection are Regulation (EC) Nr. 45/2001³ applicable to data processing by EU institutions and bodies, Directive 2002/58/EC⁴ on privacy and electronic communications and Framework Decision 2008/977/JHA⁵ on data protection in the area of police and judicial cooperation in criminal matters.
5. Under the Lisbon Treaty, data protection has gained significant importance. Not only has the Charter of Fundamental Rights of the European Union become binding but – also Article 16 of the Treaty on the Functioning of the European Union (TFEU) was introduced as a new legal basis for data protection applicable to all processing of personal data, in the private and in the public sector, including the processing in the area of police and judicial cooperation and common foreign and security policy. Article 16 gives an impetus for data protection.

¹ ETS No. 108, 28.01.1981.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281, p. 31.

³ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8, p. 1.

⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37; as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

⁵ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ 2008 L 350, p. 60., to be implemented in national law before 27 November 2010.

6. In this context, also the 'Stockholm Programme' must be mentioned. This multi-annual programme of the EU dedicates much attention to data protection in an area of Freedom, Security and Justice protecting the citizen.⁶

Central message

7. The consultation by the Commission comes at an appropriate moment, because of the important new challenges provoked by new technologies and globalisation but also in the perspective of the Lisbon Treaty.
8. The central message is that the main principles of data protection are still valid despite these important challenges. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:
 - Clarify the application of some key rules and principles of data protection (such as consent and transparency).
 - Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
 - Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
 - Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

2. One comprehensive framework

The present legal framework

9. Data protection was introduced into the legal framework of the European Union as an internal market related issue. Directive 95/46/EC is based on Article 95 EC. The purpose of this directive is twofold. The establishment and functioning of an internal market requires that personal data should be able to flow freely from one Member State to another, while at the same time a high level of protection of fundamental rights of individuals should be safeguarded.
10. Directive 95/46/EC is meant as a general legal framework, which could be complemented by specific regimes for data protection for specific sectors. Until now, only one specific regime has been adopted, for ePrivacy (currently Directive 2002/58/EC). Moreover, several pieces of sectoral legislation also contain specific rules relating to the processing of personal data (⁷ on money laundering, customs legislation or VIS, EURODAC or SIS II legislations).

⁶ The Stockholm Programme: An open and secure Europe serving and protecting the citizen, to be approved by European Council in December 2009.

⁷ E.g. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ 2005, L 309, p. 15 and the various legal instruments for the large scale information systems SIS, VIS and EURODAC.

11. The use of Article 95 EC had a consequence for the scope of application of Directive 95/46/EC. Although the Directive was meant as a general framework for data protection and in many aspects functions as such, it does not cover the processing by EU-institutions, nor processing operations that fall outside of the former first pillar (mainly the former third pillar). For the processing by the EU-institutions (as far as they operate within the former first pillar), Regulation 45/2001 was adopted which is to a large extent similar to Directive 95/46/EC. The current situation in the former third pillar can be described as a patchwork of data protection regimes, which are applicable in different situations. Some differences in these regimes stem from the specificities of the area covered, others are merely the consequence of a different legislative history. Framework Decision 2008/977/JHA can be seen as a first step towards a more general framework.
12. The situation is not satisfactory, in particular for the third pillar:
 - Data protection is now increasingly recognised as a general concern of the European Union, not necessarily linked to the internal market. This is for instance reflected in Article 8 of the Charter of Fundamental Rights of the European Union.
 - In recent years, and certainly after the terrorist attacks in the USA on 11/9/2001, the exchange of personal data between the Member States has become an essential part of police and judicial cooperation which, of course, requires appropriate protection.
 - The former division between the pillars does not reflect the reality of data protection where personal data are used in cross pillar situations, as illustrated by the PNR and Data Retention judgements of the European Court of Justice, on cases of use for law enforcement purposes of information collected originally in a business context. .

The need for a new framework

13. The shortcomings of the present system require a reflection on ‘a comprehensive and consistent data protection framework covering all areas of EU competence’⁸. The Lisbon Treaty foresees a new horizontal approach to data protection and privacy and provides for the necessary legal basis (Art. 16 TFEU)⁹ to get rid of the existing differences and divergences which prejudice a seamless, consistent and effective protection of all individuals.
14. The main safeguards and principles should apply to data processing in all sectors, ensuring an integrated approach as well as a seamless, consistent and effective protection.
15. Directive 95/46/EC should serve as a benchmark for the comprehensive framework which has as main goal effectiveness and effective protection of individuals. The existing principles of data protection need to be endorsed, and complemented with

⁸ Wording used by Commission in COM 262 Final.

⁹ Article 16 TFEU does not only extend to the third pillar, but also to the second pillar (common foreign and security policy) as far as EU institutions process personal data. Article 39 TEU provides for a specific legal basis for data processing by the Member States in the second pillar. This all is relevant for instance in relation to the terrorists' lists established by the EU and the Member States, but will not be specifically addressed in this chapter.

measures to execute these principles in a more effective manner (and to ensure a more effective protection of citizens' personal data).

16. The main principles of data protection should be the backbone of a comprehensive framework: key notions (who/data controller - what /personal data) and principles should be reaffirmed, including notably the principles of lawfulness, fairness, proportionality, purpose limitation, transparency, and rights of the data subject, as well as independent supervision by public authorities. Rethinking the framework is also an opportunity to clarify the application of some key concepts, such as:
 - consent: confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis (see also Chapter 5);
 - transparency: it is a pre-condition to fair processing. It must be clear that transparency does not necessarily lead to consent but is a pre-condition for a valid consent and the exercise of the rights of the data subject (see also Chapter 5).

The objective should be to improve data protection on an international level, in line with the principles and rights defined by Directive 95/46/EC, whilst, at the same time, upholding the current level of protection (see also Chapter 3).

17. The adoption of one comprehensive framework would also allow some useful innovations of the current rules. This might well involve the introduction of the general principle of 'privacy by design' as extension of the current rules on organisational and technical security measures (see also Chapter 4) and the general principle of accountability (see also Chapter 6).

The architecture of a comprehensive framework

18. One comprehensive framework - under the Lisbon Treaty based on a single legal basis - does not necessarily mean that there is no room for flexibility and differences between the sectors and between the Member States, within the scope of the general framework. Specific rules (*leges speciales*) could be complementary and enhance the protection, provided that they fit within the notion of a comprehensive framework and comply with the main principles, as mentioned above.
19. Additional sectoral and specific regulations could be envisaged, for example with regard to:
 - Specific sectors, such as for instance public health, employment or intelligent transport systems.
 - Privacy tools and services, such as seals and audits (see also Chapters 4 and 6).
 - Security breaches (as complement of the security principle; see also Chapters 5 and 6).
 - Police and judicial cooperation, as explicitly foreseen in Declaration 21 attached to the Lisbon Treaty (see further Chapter 8).
 - National security policy, as explicitly foreseen in Declaration 20 attached to the Lisbon Treaty.

20. Additional national regulations could be envisaged, taking into account cultural differences and the internal organisation of the Member States, provided that they do not prejudice the harmonisation, needed within a European Union without internal borders.
21. Further harmonisation is needed as part of an unambiguous and unequivocal legal framework, but this does not exclude that some flexibility can have additional value, as is presently recognised under Directive 95/46/EC for instance if needed because of cultural differences. One could also leave room for national law, to determine the allocation of responsibilities and to recognise different roles of the public and private sectors.

3. Globalisation

Context and present legal framework

22. Under EU law, data protection is a fundamental right, protected under Article 8 of the Charter of Fundamental Rights of the European Union (see also Chapter 1). In other parts of the world, the need for data protection is widely recognised but not necessarily with the status of a fundamental right.
23. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union.
24. Directive 95/46/EC has addressed this need for protection in its Article 4. The directive is applicable to data processing anywhere, and therefore also outside the EU¹⁰ (a) when the controller is established in the EU, and (b) when the controller is established outside the EU but uses equipment in the EU.
25. In addition, Article 25 and 26 of Directive 95/46/EC include a specific regime for the transfer of personal data to third countries. The basic rule of Article 25 is that transfer is only allowed to third countries that ensure an adequate level of protection. Article 26 foresees a number of derogations from this requirement. Well known concepts such as Bindings Corporate Rules (BCRs) and Standard Contractual Clauses implement this provision.

Applicable law

26. The exact scope of Directive 95/46/EC however is not sufficiently clear. It is not always clear whether EU law is applicable, which Member State law is applicable, and what would be the law(s) applicable in case of multiple establishments of a multinational in different Member States. Article 4 of the directive, determining when the directive is applicable to data processing, leaves room for different interpretation.
27. Moreover, there are situations which fall outside the scope of application of the directive. This is the case where non-EU established controllers direct their activities to EU residents which result in the collection and further processing of personal data.

¹⁰ In this context, EU should be understood as including the EFTA-countries.

For example, this is the case of on-line vendors and the like using specific advertisement with local flavor, websites that directly target EU citizens (by using local languages, etc). If they do so without using equipment in the EU, then Directive 95/46/EC does not apply.

28. At the moment, the WP29 is writing an opinion on the concept of applicable law. The WP29 envisages advising the European Commission on this topic in the course of the upcoming year. This advice might include further recommendations for a future legal framework.

International standards and the Madrid Resolution

29. Global standards regarding data protection are becoming indispensable. Global standards would also facilitate transborder data flows which, due to globalisation, are becoming the rule rather than the exception. As long as global standards do not exist, diversity will remain. Transborder data flows have to be facilitated whilst, at the same time, ensuring a high level of protection of personal data when they are transferred to and processed in third countries.
30. The ‘Madrid Resolution’, a Joint Proposal on International Standards for the Protection of Privacy which has been adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009, deserves support. The Joint Proposal contains a draft of a global standard and brings together all the approaches possible in the protection of personal data and privacy, integrating legislation from five continents. It includes a series of principles, rights and obligations that should be the basis for data protection in any legal system all over the world, and demonstrates that global standards providing an adequate level of data protection are feasible in due course.
31. The Commission is called upon:
 - To take initiatives towards the further development of international global standards regarding the protection of personal data with a view to promote an international framework for data protection and therefore facilitate transborder data flow while ensuring an adequate level of protection of data subjects. These initiatives should include investigating the feasibility of a binding international framework.
 - In the absence of global standards, to promote the development of data protection legislation providing an adequate level of protection, and the foundation of independent DPAs, in countries outside the European Union. The basic principles for data protection, as laid down in the ‘Madrid Resolution’, should be the universal basis for such legislation.

These specific tasks of the Commission should be mentioned in the future legal framework.

Improving adequacy decisions

32. Ever more processing operations of personal data take place in a globalised environment. Ensuring the free flow of personal data, while guaranteeing the level of protection of individuals’ rights, is an increasing demand. Thus, it is necessary to redesign the adequacy process:

- Defining more precisely the criteria for reaching the legal status of ‘adequacy’, paying due attention to the approach of the WP29¹¹ and various other approaches to data protection around the world, and especially to the rights and principles laid down in the Joint Proposal of International Standards on the Protection of Privacy.
- Streamlining the procedures for the analysis of the legal regimes of third countries in order to take more decisions on the adequate level of protection.

The future legal framework should specify these issues.

International agreements

33. Note has been taken of the activities of the EU-US High Level Contact Group on information sharing and privacy and personal data protection. These activities might lead to a transatlantic agreement with common principles for privacy and data protection applicable to the exchange of information with the United States for the fight against terrorism and serious transnational crime.¹²
34. International agreements are appropriate instruments for the protection of personal data in a global context, provided that the level of protection afforded is at least equivalent to the global standards mentioned above, that every individual has an easy and effective redress, including judicial redress, and that specific safeguards are included relating to the purpose for which the personal data will be used.
35. Under those conditions the foreseen transatlantic agreement could serve as a model for exchange with other third countries and for other purposes. The future legal framework could mention the conditions for agreements with third countries.
36. Furthermore, the EU should encourage the cooperation between international data protection authorities, for example on a transatlantic level. Such cooperation is a successful means to promote data protection outside the EU.

Binding Corporate Rules / Accountability

37. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs), international codes of conduct for multinationals, allowing for the worldwide transfer within a multinational corporation. BCRs have been introduced by the WP29 in 2003. Both DPAs and multinationals are of the opinion that BCRs are a good means to facilitate international data flows whilst guaranteeing the protection of personal data. However, Directive 95/46/EC did not expressly take account of BCRs. As a result the process for adoption of BCRs, which is based on Article 26 (2) of Directive 95/46/EC, requires the approval of all Member States concerned by a BCR. As a result, assessing and approving BCRs takes a long time. The WP29 has devoted considerable effort to promote and facilitate the use and the approval of BCRs within the current legal framework. In order to improve the process, so far, nineteen DPAs have agreed to a procedure on the approval of BCRs called ‘Mutual Recognition’.

¹¹ See in particular WP 29 Working Document 12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, adopted on 24 July 1998

¹² In this regard, the transatlantic problem regarding redress remains to be solved.

38. Against this background a provision on BCRs should be further reinforced and included in the new legal framework, which would serve several purposes:
- Recognising BCRs as appropriate tool to provide adequate safeguards.
 - Defining the main substantive and procedural elements of BCRs, following the WP29 Opinions on the subject.
39. Moreover, from a general point of view, a new provision could be included in the new legislative framework pursuant to which data controllers would remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU (see on 'accountability' more in general Chapter 6).

Final remark

40. This chapter discusses globalisation as such. However, in one way or another, all chapters of this contribution deal with this subject. Often, when one thinks of 'globalisation', one thinks of business. However, increasingly processing operations of personal data take place in a globalised world. Even though the individual often lives a local life, he can more and more be found on line where his data are processed globally. Globalisation therefore is linked to technology (Chapter 4), the position of the data subject (Chapter 5), data controller (Chapter 6), DPAs / WP29 (Chapter 7) and law enforcement (Chapter 8).

4. Technological changes; Privacy by Design as a new principle

41. The basic concepts of Directive 95/46/EC were developed in the nineteen seventies, when information processing was characterized by card index boxes, punch cards and mainframe computers. Today computing is ubiquitous, global and networked. Information technology devices are increasingly miniaturized and equipped with network cards, WiFi or other radio interfaces. In almost all offices and family homes users can globally communicate via the Internet. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects.
42. Directive 95/46/EC has stood well the influx of these technological developments because it holds principles and uses concepts that are not only sound but also technologically neutral. Such principles and concepts remain equally relevant, valid and applicable in today's networked world.
43. While it is clear that technological developments described above are generally good for society, nevertheless they have strengthened the risks for individuals' privacy and data protection. To counterbalance these risks, the data protection legal framework should be complemented. First, the principle of 'privacy by design' should be introduced in the new framework; second, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

Privacy by design principle

44. The idea of incorporating technological data protection safeguards in information and communication technologies ('ICT') is not completely new. Directive 95/46/EC already contains several provisions which expressly call for data controllers to implement technology safeguards in the design and operation of ICT. This is the case of Article 17 which lays down the data controllers' obligation to implement appropriate technical and organizational measures. Recital 46 calls for such measures to be taken, both at the time of the design of the processing system and at the time of the processing itself. Article 16 establishes the confidentiality of processing, a rule which is mirrored and complemented in regulations regarding IT security. Apart from these articles, the principles relating to data quality as contained in Article 6 (lawfulness and fairness, purpose limitation, relevance, accuracy, time limit of storage, responsibility) also apply.
45. Whereas the above provisions of the Directive are helpful towards the promotion of privacy by design, in practice they have not been sufficient in ensuring that privacy is embedded in ICT. Users of ICT services – business, public sector and certainly individuals – are not in a position to take relevant security measures by themselves in order to protect their own or other persons' personal data. Therefore, these services and technologies should be designed with privacy by default settings.
46. It is for these reasons that the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements.
47. Such principle should call for the implementation of data protection in ICT (privacy by design or 'PbD') designated or used for the processing of personal data. It should convey the requirement that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed. This is in line with recent case law in Germany.¹³
48. The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption). It should be a crucial requirement for products and services provided to third parties and individual customers (eg. WiFi-Routers, social networks and search engines). In turn, it would give DPAs more powers to enforce the effective implementation of such measures.

¹³ Recently the German Constitutional Court (Judgment of 27 February 2008 – [1 BvR 370/07](#); [1 BvR 595/07](#) –) created a constitutional right in the confidentiality and integrity of information technology system. Systems that are able to create, process or store sensitive personal data require special protection. The protective scope of the fundamental right in confidentiality and integrity of information technology system is applied to systems which alone, or in their technical interconnectedness, can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of their personality. These systems are for example personal computers and laptops, mobile phones and electronic calendars.

49. Such principle should be defined in a *technologically neutral* way in order to last for a long period of time in a fast changing technological and social environment. It should also be *flexible* enough so that data controllers and DPAs will, on a case by case basis, be able to translate it in concrete measures for guaranteeing data protection.
50. The principle should emphasize, as current Recital 46 does, the need for such principle to be applied *as early as possible*: 'At the time of the design of the processing system and at the time of the processing itself'. Safeguards implemented at a late stage are inconsistent and insufficient as regards the requirements of an effective protection of the rights and freedoms of the data subjects.
51. Technological standards should be developed and taken into consideration in the phase of system analysis by hardware and software engineers, so that difficulties in defining and specifying requirements deriving from the principle of 'privacy by design' are minimized. Such standards may be general or specific with regard to various processing purposes and technologies.
52. The following examples demonstrate how PbD can contribute to a better data protection:
 - Biometric identifiers should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases.
 - Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence.
 - Patient names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment.
 - Where appropriate, functionality should be included facilitating the data subjects' right to revoke consent, with subsequent data deletion in all servers involved (including proxies and mirroring).
53. In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected:
 - Data Minimization: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
 - Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
 - Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.

- User Friendly Systems: privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- Data Confidentiality: it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
- Data Quality: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- Use Limitation: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

Regulations for specific technological contexts

54. The privacy by design principle may not be sufficient to ensure, in all cases, that the appropriate technological data protection principles are properly included in ICT. There may be cases where a more concrete 'hands on approach' may be necessary. To facilitate the adoption of such measures, a new legal framework should include a provision enabling the adoption of specific regulations for a specific technological context which require embedding the privacy principles in such context.
55. This is not a new concept; Article 14 (3) of the ePrivacy Directive, contains a similar provision: 'Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and communications)'.¹⁴
56. The above would facilitate the adoption, in specific cases, of specific legislative measures embedding the concept of 'privacy by design' and ensuring that adequate specifications are provided. For example, this may be the case with RFID technology, social networks, behavioral advertisement, etcetera.

Final remarks

57. The increasing significance of data protection when creating and operating IT-systems is posing additional requirements to IT-specialists. This causes the need to firmly incorporate data protection into the curricula of IT-professions.
58. The technological data protection principles and the ensuing concrete criteria should be used as a basis for awarding labels of quality (certification schemes) in a framework of a data protection audit.¹⁴

5. Empowering the Data Subject

59. The potential of the position of the data subject in Directive 95/46/EC has not been fully used. In addition, both the behaviour of citizens and the role of data subjects with respect to data protection have changed, amongst others due to sociological

¹⁴ For example, this is the case with the EuroPriSc project.

changes and new ways of data collection (for instance for profiling purposes). Data subjects can be careless with their own privacy, are sometimes willing to trade privacy for perceived benefits. On the other hand, they still have high expectations of those with whom they do business. Also, data subjects themselves more and more play an active role in the processing of personal data, in particular on the internet.

60. Changes in the behaviour and role of the data subject and the experience with Directive 95/46/EC require a stronger position for the data subject in the data protection framework.¹⁵ Further empowerment of the data subject in order to be able to play a more active role is essential.

Improving redress mechanisms

61. Empowerment of the data subject requires giving the data subject more options to execute and enforce his rights. As court proceedings can sometimes be very difficult and bear a financial risk, the possibility for class action procedures should be introduced in Directive 95/46/EC.¹⁶
62. In addition, data controllers should provide for complaints procedures which are more easily accessible and more effective and affordable (see also Chapter 6). If these procedures do not resolve the dispute between data subject and data controller, the data subject should be able to turn to alternative dispute resolutions, primarily provided for by the industry.¹⁷ These options should be included in the new legislative framework.

Transparency

63. Transparency is another fundamental condition, as it gives the data subject a say in the processing of personal data, 'ex ante', prior to processing. Profiling, data mining, and technological developments which ease the exchangeability of personal data make it even more important for the data subject to be aware by whom, on what grounds, from where, for what purposes and with what technical means data are being processed. It is important that this information is understandable. However, the duty to inform the data subject (Articles 10 and 11 of Directive 95/46/EC) is not always properly put into practice. A new legal framework should provide alternative solutions, in order to enhance transparency. For example, new ways to inform data subjects could be developed in relation to behavioural advertising.
64. In addition, transparency requires that affected individuals should be notified when a privacy breach which is likely to adversely affect their personal data and privacy occurs. That would enable the data subjects to try and control the damage that has been inflicted upon them (in certain cases authorities should be notified as well, see also Chapter 6). A general privacy breach notification should be introduced in the new legal framework (see also Chapter 6).¹⁸

¹⁵ This is especially the case when it concerns children. When taking decisions about their personal data, their best interest needs to be a primary consideration, as stated in the UN Convention on the Rights of the Child (<http://www2.ohchr.org/english/law/crc.htm>) and other specific international instruments and national law.

¹⁶ Class actions for example exist in environmental law.

¹⁷ This may of course not deprive an individual from a proper redress before a Court or a DPA.

¹⁸ In 'Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)' the WP29 has noted a recommended approach to the issue of the specific privacy breach notifications which are taken on board in the ePrivacy Directive. The same recommendations apply to the introduction of general privacy breach notifications.

Consent

65. In the Directive, consent of the data subject is a legitimate ground for data processing (Article 7 and 8 of Directive 95/46/EC). It is and continues to be an important ground for processing, which could under certain circumstances empower the data subject. However, consent needs to be freely given, informed and specific (Article 2 (h) of Directive 95/46/EC).
66. There are many cases in which consent can not be given freely, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities).
67. In addition, the requirement that consent has to be informed starts from the assumption that it needs to be fully understandable to the data subject what will happen if he decides to consent to the processing of his data. However, the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice.¹⁹
68. In both hypotheses, consent is an inappropriate ground for processing but nevertheless often falsely claimed to be the applicable ground. The technological developments also ask for a careful consideration of consent. In practice, Article 7 of Directive 95/46/EC is not always properly applied, particularly in the context of the internet, where implicit consent does not always lead to unambiguous consent (as required by Article 7 (a) of the Directive). Giving the data subjects a stronger voice 'ex ante', prior to the processing of their personal data by others, however requires explicit consent (and therefore an opt-in) for all processing that is based on consent.²⁰
69. The new legal framework should specify the requirement of consent, taking into account the observations made above.

Harmonisation

70. Currently the empowerment of data subjects is being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Several elements of the Directive which are of essence to the position of data subjects, such as the liability provision and the possibility to claim immaterial damages,²¹ have not been implemented by all Member States. Besides these differences in the implementation of Directive 95/46/EC, the interpretation of the Directive in the Member States is not always uniform. As globalisation increases, these differences

¹⁹ See 'Data Protection Accountability: The essential Elements – A Document for Discussion', Centre for Information Policy Leadership, as Secretariat to the Galway Project, October 2009, p.4.

²⁰ Regarding consent and opt-in / opt-out, see also chapter 2, where it is stated that confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis.

²¹ In the majority of cases in which damage has been inflicted upon the data subject, the damage consists of immaterial damage such as the sense no longer to be able to move through the public and private sector without being watched. This problem increases in the current 'surveillance society'.

more and more weaken the position of the data subject. It is therefore of great importance that harmonisation be improved (see also Chapter 7b), if needed by specifying legislative provisions.

The role of data subjects on the internet

71. Increasingly, individuals upload their own personal data into the internet (social networks, cloud computing services, etc). However, Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'.²² Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller.²³ The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller. In addition, thought should be given to the question whether data subjects should be given more means to execute their rights on the internet, including the protection of rights of third parties whose personal data may be object of processing (e.g. social networks). As there are many more unresolved issues in this context,²⁴ the role of the data subject on the internet should be further clarified, in view of a new legal framework.

6. Strengthening Data Controllers' Responsibility

72. Under Directive 95/46/EC, the data controller is the key actor to ensure compliance with the principles and obligations aimed at safeguarding the protection of personal data of individuals. The Directive, implicitly and in many cases explicitly, requires the data controller to respect data protection principles and fulfil certain specific obligations.²⁵ Examples of the latter include notifying and prior checking of data processing operations with national authorities.²⁶ Furthermore, ensuring respect for individuals' data protection rights requires the imposition of corresponding duties upon the data controller such as the provision of information.²⁷

²² For a better understanding of whether an activity is covered or not by this 'household exemption', see [Opinion 5/2009](#), on online social networking (WP 163).

²³ This problem does not arise where organizations - either in public or private sector - make use of cloud computing applications, since the Directive applies to them and their processing operations where "carried out in the context of the activities of an establishment of the controller" in the EU (see Article 4.1.a). Chapter 5 thus applies to them, regardless of whether the service provider is established in the EU or not.

²⁴ Regarding, for example, the consent of children and/or their parents, access requests by law enforcement, access rights to internet accounts by heirs of deceased people, and third party applications.

²⁵ Article 6 (2) explicitly provides that "it shall be for the controller to ensure that paragraph 1(which refers to the main principles relating to data quality) "is complied with".

²⁶ See Articles 18-21 of Directive 95/46.

²⁷ Other examples of data subjects' rights include the right to access, rectification, erasure and blocking, and to object to the processing of personal data (Articles 10-12 and 14). These rights entail obligations for the controller to satisfy them.

73. These obligations also apply - directly or indirectly - to data processors when/if data controllers have entrusted all or part of the data processing operations to them. To provide guidance on the concept of data controller and processor, the WP29 is currently engaged in drafting an interpretative opinion. The WP29 envisages to soon advise the Commission on this topic. This advice might include further recommendations for a future legal framework.

Embedding data protection in organisations

74. The relevant provisions of Directive 95/46/EC form an undeniably solid base for the protection of personal data and should be maintained. Nonetheless, compliance with existing legal obligations often is not properly embedded in the internal practices of organizations. Frequently, privacy is not embedded in information processing technologies and systems. Furthermore, management, including top level managers, generally are not sufficiently aware of and therefore actively responsible for the data processing practices in their own organizations. The data protection scandals that have taken place in some Member States in the last few years support this concern.

75. Unless data protection becomes part of the shared values and practices of an organization, and unless responsibilities for it are expressly assigned, effective compliance will be at risk and data protection mishaps will continue. In turn, this may undermine public trust and confidence in business and public administrations alike. Moreover, embedding data protection in organizations' cultures will assist national DPAs in their supervision and enforcement tasks, as further developed in Chapter 7, strengthening the effectiveness of privacy protections.

76. The principles and obligations of Directive 95/46/EC should permeate the cultural fabric of organizations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department. The Directive's requirements should result in concrete data protection arrangements being applied on a day-to-day basis. Privacy controls should be integrated into the design of information technologies and systems (see also Chapter 4). Furthermore, within the organizations, both in public and private sectors, internal responsibility for data protection should be properly recognized, strengthened and specifically assigned.

77. The effectiveness of the provisions of Directive 95/46/EC is dependent on data controllers' effort towards achieving these objectives. This requires the following proactive measures:

- *Adoption by data controllers of internal policies and processes* to implement the requirements of the Directive for the particular processing operations carried out by the controller. Such internal policies and processes should be approved at the highest level within the organization and therefore be binding for all staff members.
- *Putting in place mechanisms executing the internal policies and processes, including complaints procedures (see also Chapter 5)*, in order to make such policies effective in practice. This may include creating data protection awareness, staff training and instruction.
- *Drafting compliance reports and carrying out audits, obtaining third-party certification and/or seals* to monitor and assess whether the internal measures adopted to ensure compliance effectively manage, protect, and secure personal data (see also Chapter 4).

- Carrying out *privacy impact assessments*, particularly for certain data processing operations deemed to present specific risks to the rights and freedoms of data subjects, for example, by virtue of their nature, their scope or their purpose.
- *Assignment of responsibility for data protection* to designated persons with direct responsibility for their organizations' compliance with data protection laws.
- *Certification of compliance by top level company executives* confirming that they have implemented appropriate safeguards to protect personal data.
- *Transparency of these adopted measures vis-à-vis the data subjects and the public in general.* Transparency requirements contribute to the accountability of data controllers (e.g. publication of privacy policies on the internet, transparency in regard to internal complaints procedures, and publication in annual reports).

78. Article 17 (1) of Directive 95/46/EC, to some extent, already requires data controllers to implement measures, of both technical and organizational nature (the data controller must “*implement appropriate technical and organizational measures to protect personal data against... unlawful forms of processing*”). These measures may include some of the above measures. However, in practice Article 17 (1) has not been successful in making data protection sufficiently effective in organizations, also due to different approaches taken in the national implementing measures.

Accountability principle²⁸

79. To address this problem, it would be appropriate to introduce in the comprehensive framework an accountability principle. Pursuant to this principle, data controllers would be required to carry out the necessary measures to *ensure* that substantive principles and obligations of the current Directive *are observed* when processing personal data. Such provision would reinforce the need to put in place policies and mechanisms to make effective the substantive principles and obligations of the current Directive. It would serve to reinforce the need to take effective steps resulting in an internal effective implementation of the substantive obligations and principles currently embedded in the Directive. In addition, the accountability principle would require data controllers to have the necessary internal mechanisms in place to *demonstrate compliance* to external stakeholders, including national DPAs. The resulting need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate the enforcement of applicable rules.

80. In any event, the measures expected from data controllers should be scalable and take into consideration the type of company, whether large or small, and of limited liability, the type, nature and amount of the personal data by the controller, among other criteria.

More options: proactive or reactive

81. Some of the measures described above could be deemed as standard good practice, thus fulfilling the accountability principle if carried out in practice. A built-in reward structure could be foreseen in law to induce organizations to implement them.

²⁸ See on accountability also Par. 39.

82. An alternative solution could be more prescriptive. For example, Article 17 (1) could be elaborated in order to specify additional proactive measures, such as those outlined above, to be implemented by data controllers. These measures should be orientated towards achieving specific outcomes and should be technologically neutral.
83. Other measures would be of a more reactive nature. They would apply when there has been an unlawful processing of personal data and might, inter alia, involve the following:
- *Setting up a mandatory security breach notification obligation* (see also Chapters 2 and 5).
 - *Reinforcement of enforcement powers of DPAs*, including the imposition of concrete requirements to ensure an effective protection (see also Chapter 7a).

Simplification of notifications

84. Notifications of data processing operations with national DPAs could be simplified or diminished. In this context, the link between compliance with the requirements mentioned above and the possibility to further nuance the administrative requirements, in particular the notification of data processing activities with national DPAs, should be explored.
85. Notification contributes to the awareness of the data processing operations and data protection practices within organizations.²⁹ It also gives DPAs an overview of data processing activities. However, better data governance and accountability requirements may achieve the same purposes. Those mechanisms might help to carry out the necessary measures to observe the substantive principles and obligations currently embedded in the Directive and to produce evidence of such compliance.
86. It should be explored whether and to what extent notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases. Even in such cases, notification could be streamlined, for example, by providing the results of privacy impact assessments, or the outcome of third-party auditing. This could be combined with a registration system whereby all data controllers would be enrolled in a registry maintained by the DPA, to ensure the easy identification of organizational entities for efficient and effective enforcement when necessary.

7. Stronger and clearer roles for DPAs and their cooperation within the EU

7a. Data Protection Authorities

87. At the moment, there are big differences regarding the position of the DPAs in the 27 Member States. This is due to the differences in history, case law, culture and the internal organization of the Member States, but also because Article 28 of Directive

²⁹ These views are further confirmed by the WP's report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union (WP 106), adopted on 18 January 2005.

95/46/EC lacks precision in several aspects. On top of that, the Directive has, to a certain extent, been poorly implemented in some jurisdictions. This has resulted in large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs.

88. The new challenges to data protection (globalisation and the technological changes, Chapters 3 and 4) require strong supervision by DPAs, in a more uniform and effective way. As a consequence, the new framework should guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.
89. DPAs need to be fully and truly independent. The current Article 28 (1) of Directive 95/46/EC is unclear in this respect as is demonstrated by Case C-584/07 (Commission v. Germany), currently before the European Court of Justice. In the new legal framework DPAs should have:
 - complete institutional independence and not be subordinated to any other government authority.
 - functional independence and not be subject to instructions by the controlled, in relation to the contents and extent of its activity.
 - material independence. They should have an infrastructure which is suited to the smooth conduct of their activities, in particular adequate funding. Sufficient resources should be allocated to the DPAs.
90. The enforcement role of DPAs is becoming increasingly important. DPAs need to be able to be strong and bold, and strategic on intervention and enforcement. The current wording of article 28 of Directive 95/46/EC has resulted in widely diverse enforcement powers. The new framework should require a more uniform approach from Member States in giving the DPAs the necessary powers and it should be more specific in this regard than Directive 95/46/EC. The necessary powers should, amongst others, include the power to impose financial sanctions on controllers and processors.
91. The advisory role of DPAs in the legislation making process is indispensable, as the knowledge that DPAs acquire from investigation and enforcement actions often is necessary in order to improve (data protection) legislation. The advisory role should involve all measures and regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, not just 'administrative measures and regulations'³⁰. DPAs should be asked for advice before the draft legislation is adopted. In addition, the new framework should ensure that DPAs have an advisory role towards their national Parliaments and/or other national competent institutions, at the time when the latter are involved in the drafting process of new EU legislation.
92. DPAs need to be able to fix their own agenda when setting priorities with regard to, inter alia, the handling of complaints, including the manner in which complaints are handled.³¹ DPAs should in any case be able to take into account whether the

³⁰ Article 28 (2) of Directive 95/46/EC.

³¹ The possibility to be selective can be put in practice in different ways, e.g. by establishing 'fast track' procedures to deal with minor claims.

handling of a certain complaint will sufficiently contribute to the protection of personal data.³² The new framework should enable the DPAs to ‘be selective to be effective’.

93. On the other hand, DPAs need to be accountable for the way they make use of their stronger supervisory role. They should be transparent in this regard and publicly report on the way they operate and the priorities they set. The current wording of Article 28 (5) of Directive 95/46/EC needs to be specified in this regard in the new framework.

7b. Cooperation of Data Protection Authorities

The present legal framework

94. Article 29 of Directive 95/46/EC has set up the Working Party on the protection of individuals with regard to the processing of personal data (WP29) as the institutional body for cooperation among national DPAs. The WP29 has an advisory status and acts independently. Its tasks are set forth in Article 30 (1) of the Directive and include contributing to the uniform application of the Directive, by examining questions covering the application of the national measures, giving opinions on the level of protection in the Community and in third countries, as well as advising (also on its own initiative) on proposals for Community legislation having an impact on data protection or any other matters relating to the protection of persons with regard to the processing of personal data in the Community. The Commission is a member of the WP29 and provides for the Secretariat.
95. The WP29 fulfils its task within the scope of Directive 95/46/EC, as specified in its Article 3 (2). In the area of police and judicial cooperation, the European DPAs have established in 2007 the Working Party on Police and Justice (WPPJ) which fulfils a similar role as WP29, but without a legal basis and a secretariat provided for by an EU Institution. Framework Decision 2008/977/JHA, which introduces data protection principles in that area, does not provide for any institutionalised cooperation of DPAs.

The functioning of the WP29

96. The WP29 now functions for over 10 years and has significantly contributed to achieve the goals of Article 30 of Directive 95/46/EC. The result of many of its activities can be found on its website.³³
97. The WP29 has constantly worked on how to improve its effectiveness and should continue to pay attention to its own functioning.
Special points of consideration are:
- how can the WP29 effectively contribute to the uniform implementation of EU legislation in national laws and to the uniform application of national law?

³² Criteria which can be applied to determine whether a complaint should be handled are for example whether the complaint relates to a situation which affects a large number of people, concerns a breach of data protection legislation which is not of little importance and probably not an incidental phenomenon, and whether handling the complaint is likely to be successful and does not require disproportionate efforts.

³³ http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue

- how can it improve its effectiveness vis-à-vis the EU institutions and in particular the Commission, also taking into account the hybrid role of the Commission as member of the WP29, as its secretariat as well as the addressee of many of the opinions of the WP29?

Consequences for the future

98. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. A comprehensive legal framework should include a comprehensive advisor and an effective cooperation between supervisory authorities. In a transitional period, before a legislative change is realized, appropriate forms for the WP29 to work closely together with the WPPJ must be found.
99. Other improvements do not require a legislative change.
- The uniform application of national law implementing Directive 95/46 can be achieved within the present legal framework, by further improving the working methods of the Working Party and, where needed, by insisting on a strong commitment by the members of the WP29 to implement the views of the WP29 into national practice.
 - In accordance with Article 29 of Directive 95/46/EC, the Secretariat of the WP29 is provided by the Commission. The Secretariat should work in close cooperation with the Presidency of the WP29 and its staff. The tasks of the Secretariat and the Presidency are complementary and they should closely work together in order to enable the WP29 to fulfill its missions in the most efficient manner. While the Secretariat deals with all the logistical aspects of the work of the WP29 and assists the WP29 in preparing its opinions and documents, the Presidency (and the Vice-Presidency) focus mainly on the decision-making process and on the strategy of the WP29.
 - Relations with the Commission can be further improved by describing the main roles of both players in a Memorandum of Understanding between the WP29 and the Commission. This Memorandum should also address the resources available for the WP29 so that it can use its full capacity in assuming its assignments. Finally, it should address the functioning of the Secretariat, in order to ensure that both the WP29 and the Secretariat itself have sufficient resources to prepare the opinions and working documents of the WP29. The WP29 will enter into consultation with the Commission on the above in 2010.

8. Data protection challenges in the field of police and law enforcement

100. Data protection in the field of police and justice is a specific subject which requires specific attention, taking into account the complex relation between the activities of the State to ensure security and the protection of the personal data of the individual. The specificity of this area is not only the result of the former pillar structure of the previous EU-Treaties, but is more widely recognised (see for instance the exceptions of Article 13 of Directive 95/46/EC and Declaration 21 attached to the Lisbon Treaty).

Changing context within the EU

101. With the entry into force of the Lisbon Treaty, new perspectives will be created for law making in the field of data protection. The pillar structure will be abolished and with Article 16 TFEU a single legal basis is created for data protection in almost all areas of EU law (see Chapter 2). This does not necessarily mean that the implementation of data protection principles for police and justice should be the same as the rules in other parts of society. Declaration 21, attached to the Lisbon Treaty claims that specific rules for law enforcement area 'may prove to be necessary'.
102. Data protection and data exchange will be important focuses in the Stockholm Programme. Decision making will be based on the notion of the right balance between the needs of law enforcement and the requirements of data protection. New measures should only be taken after a proper evaluation of the existing legal framework.
103. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters must be implemented by the Member States before 27 November 2010. This Framework Decision can be seen as a first step towards a general framework in the former third pillar but is far from complete. It is only applicable in cross border situations. It seems to lack essential elements and tools to effectively deal with the changing working methods in the area of law enforcement.

Changing emphasis in law enforcement

104. The last years have shown a shift of emphasis in working methods of the police and the judicial authorities, as far as the use of (personal) information is concerned. This shift was the result of growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime and was stimulated by the technological developments over the last years.
105. The shift of emphasis has several dimensions:
- The use of information focuses on earlier stages in the chain: in addition to the traditional use of information for the investigation and the detection of a specific crime, information is gathered and exchanged in order to prevent possible criminal acts ('preventive policing').
 - The use of information focuses on a wider group of persons. Information is gathered and exchanged, not only on persons that are directly related to a crime such as suspects or witnesses, but also on wider groups of the population who are not involved in an investigation (e.g. travellers, users of payment services, etc.).
 - The information that is used is more and more technology based. Technology even links disparate factors to predict future behaviour of individuals by means of automated tools (data mining, profiling).
 - The information that is used is of a different nature. Information use relies not only on objectively determined information (hard data) but also on information based on evaluation and analysis in the framework of an investigation (soft data). Besides, the distinction between the two may vary depending on the Member States.

- The increased use for preventive purposes of personal information originating from the private sector, like for instance banking/financial data, and passenger data collected by air carriers and CRS.
- Information that is collected for a given, legitimate purpose is increasingly used for different, at times incompatible purposes and tends to growingly converge. Interoperability between systems is an important development but is not a purely technical issue, in particular in view of the risks of interconnection of databases having different purposes.
- More authorities are involved in the use of information, not just police and judicial authorities *strictu sensu* but also other public authorities like authorities responsible for border control and tax authorities, but also national security services.

106. This changing emphasis in law enforcement has led to a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector. The technological possibilities to easily combine information may have a profound impact on the privacy and data protection of all citizens and on the very possibility for them to really enjoy and be able to exercise their fundamental rights, in particular whenever freedom of movement, freedom of speech, and freedom of expression are at issue.

Challenges for data protection

107. Against this background, the challenges for data protection are immense. A future legal framework should in any event address the following phenomena:

- Tendencies may lead towards a more or less permanent surveillance of all citizens, often referred to as the surveillance society. An example would be the combined use of intelligent CCTV-camera's and other tools, like an Automatic Number Plate Recognition, registering all cars entering and exiting a certain area.
- Databases may be used for data mining, and risk assessments of individuals can be composed on the basis of profiling of individuals. This might stigmatize persons with certain backgrounds.
- Analyses made on the basis of general criteria run the risk of high inaccuracies, leading to a high number of false negatives and false positives.
- The processing of personal data of non-suspects becomes more important. Specific conditions and safeguards are needed in order to assess their legitimacy and proportionality and to avoid prejudice for persons that are not (actively) involved in a crime.
- There is an increased use of biometric data, including DNA, which presents specific risks.

Conditions for law and policy making

108. The growing number of sector-specific initiatives adopted or planned may easily lead to overlapping or even distortion measures. Therefore, there may be added value in basing information exchange on a consistent strategy, provided that data protection is fully considered and is an integrated part of this strategy.³⁴

³⁴ A European Information Management Strategy, as currently elaborated by the Council, may - if done correctly - in this context prove to be a useful instrument.

109. The need for evaluation of the existing legal instruments and their application is of utmost importance and should take into account the costs for privacy. Evaluation of existing measures should take place before taking new measures. Additionally, a periodic review of existing measures should take place.
110. Transparency is an essential element. Clear information should be available to data subjects on the use of the information collected and the logic underlying the processing and should only be limited if necessary in individual cases to not jeopardise investigations and for a limited period of time. Access and rectification rights of the data subject should be addressed in a cross border context to avoid that the data subject loses control.
111. Special attention is needed for transparency and democratic control in the legislative process. Privacy impact assessments, appropriate forms of consultation of data protection authorities and an effective parliamentary debate, at national and EU level, should play an important role.
112. The architecture of any system for storage and exchange of personal data should be well elaborated. Some general considerations are:
- Privacy by design and PETS (certification scheme) should determine the architecture. In the area of freedom, security and justice where public authorities are the main actors and every initiative aimed at increasing surveillance of individuals and increasing the collection and use of personal information could have a direct impact on their fundamental right to privacy and data protection, those requirements could be made compulsory.
 - Purpose limitation and data minimization should remain guiding principles.
 - Access to large databases must be configured in such a way that in general no direct access on line to data stored is allowed, and a hit/no hit system or an index system is in general considered preferable..
 - The choice between models with central storage, meaning systems with a central database on EU-level and decentralised storage should be made on transparent criteria and in any event ensure a solid arrangement providing for a clear definition of the role and responsibilities of the controller/s and ensuring the appropriate supervision by the competent data protection authorities.
 - Biometric data should only be used if the use of other less intrusive material does not present the same effect.
113. The external dimension. It should be avoided that the stringent regime for the exchange of personal data within the EU will be circumvented. The relations with third states should be based on a clear framework, binding on all parties and on the notion of adequacy. The adequacy regime should be assessed following an evaluation by the national DPAs, if necessary through common mechanisms ensuring consistent implementation and effectiveness.
114. Special attention - including where necessary tailor made safeguards for data protection - is needed for large scale information systems within the EU.
115. Independent supervision, as well as judicial oversight and remedies should be properly addressed. This includes in any event adequate resources and competences for independent supervision.

116. Cooperation between DPAs in charge of ensuring lawfulness of data processing should be strengthened in all matters and integrated in the legal framework, also by envisaging stable mechanisms similar to those currently applying to first pillar matters, in order to foster a harmonised approach across the EU and beyond.

For the Art 29 Working Party

For the Working Party on Police and Justice

The Chairman

The Chairman

Alex Türk

Francesco PIZZETTI

APPENDIX C

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



November 2009



THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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: 7 Foundational Principles</i>	6
V Leadership Companies are Demonstrating <i>Privacy by Design</i>	8
<i>Privacy by Design – an HP Example</i>	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.

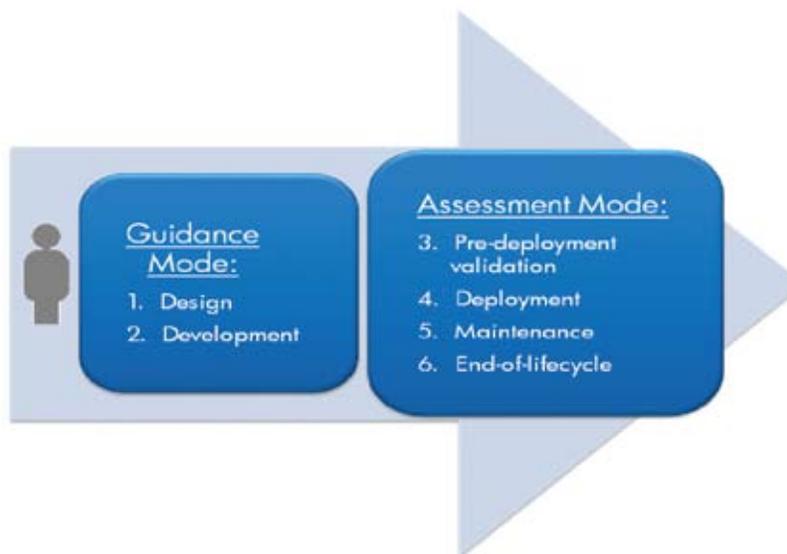
³ "Managing Global Information Privacy" is available on the OCED website (www.oecd.org) and The Privacy Projects, a NGO that sponsored the research

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
 No
 Not Sure

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

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

Customer information
 Employee information
 Other

[Help with question](#)

Question is unclear

[Help with question](#)

Question is unclear

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

BACK
SAVE AND CONTINUE
SAVE AND EXIT

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

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 Hunton & 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 - Hunton & Williams, LLP, and IPC shall not be liable for technical or editorial errors or omissions contained herein.

