
THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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

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

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

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

February 18, 2011

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

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

Dear Sirs and Madams:

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

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

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. It is located within the law firm of Hunton & Williams and is financially supported by approximately 40 member organizations. The Centre’s views and the views expressed in this response are its own and do not necessarily reflect those of its member companies, the law firm of Hunton & Williams LLP, or the firm’s clients.

Federal Trade Commission
February 18, 2011
Page 2

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 3

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

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 4

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

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

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 5

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

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 6

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

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 7

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

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

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

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

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

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

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

Federal Trade Commission
February 18, 2011
Page 8

Consumer education

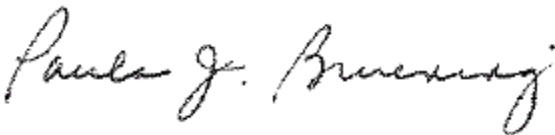
Consumer education related to privacy should be an ongoing effort of business, advocates and government. Consumer education enhances transparency by helping individuals better understand privacy notices, when choice may be an option, and when access may be available to them. Taken more broadly, consumer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

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

Respectfully submitted,



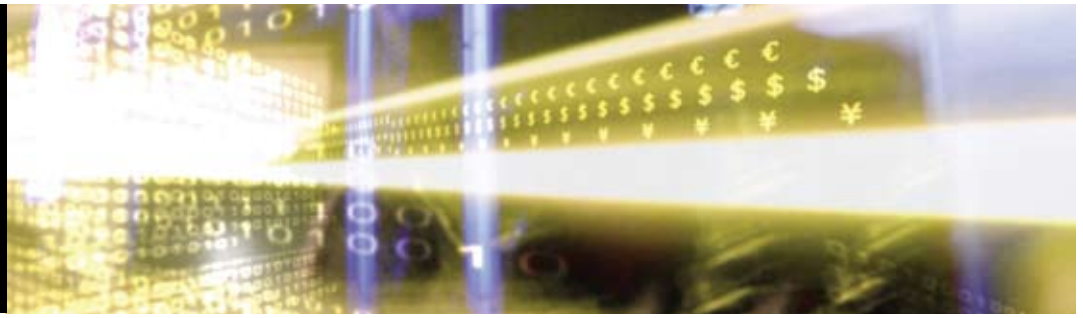
Martin E. Abrams
Executive Director



Paula J. Bruening
Deputy Executive Director

Federal Trade Commission
February 18, 2011

APPENDIX A



Demonstrating and Measuring Accountability

A Discussion Document

Accountability Phase II – The Paris Project
October 2010

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

Preface

Martin E. Abrams
Centre for Information Policy Leadership

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

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

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

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

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

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

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

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

Demonstrating and Measuring Accountability

The Accountability Project – Phase II

Paris, France

Introduction

Over the past 18 months, policymakers around the world have undertaken efforts to examine and update privacy protections in a way that better serves the needs of individuals and organisations¹ and takes into account the realities of technologies and data flows of the 21st century. The concept of accountability has figured prominently in many of these discussions.

An accountability principle has been a feature of both the earliest of the major international instruments on privacy, the Organisation for Economic Cooperation and Development's Privacy Guidelines, published in 1980,² and the most recent, the Asia Pacific Economic Cooperation's APEC Privacy Framework, endorsed in 2005.³ Both require that organisations "should be accountable for complying with measures that give effect" to the fair information practices articulated in the respective guidelines.

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

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

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

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

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

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

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

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

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

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

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

- (1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
- (2) Mechanisms to put privacy policies into effect, including tools, training and education.
- (3) Systems for internal, ongoing oversight and assurance reviews and external verification.
- (4) Transparency and mechanisms for individual participation.
- (5) Means for remediation and external enforcement.⁸

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

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

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

The Scope of Accountability and Benefits to Organisations

A General Requirement of Accountability

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

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

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

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

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

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

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

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

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

A Customized Approach

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

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

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

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

The Role of Certification - Review and Acceptance of Practices

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

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

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

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

Demonstrating Accountability

For What Are Organisations Accountable?

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

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

To Whom Are Organisations Accountable?

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

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

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

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

Common Fundamentals of an Accountability Implementation Program

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Measuring Accountability

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

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

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

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

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

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

1. The organisation takes appropriate measures to establish processes and procedures that implement its privacy policies. It carries out risk analysis and mitigation based on their understanding of its obligations under an accountability approach. The organisation may enlist the consultation of the supervisory authority or recognized accountability agent in this process and complete the appropriate documentation.
2. The organisation self-certifies that it meets the requirements of accountability.
3. The supervisory authority or recognized accountability agent reviews such filings and provides some form of acceptance of the certification.
4. The organisation submits to enforcement by the supervisory authority or recognized accountability agent. The supervisory authority or accountability agent will hear and resolve complaints from individuals. It will also conduct appropriate organisation spot checks to ensure that they continue to meet the criteria to which they have self-certified.¹⁵
5. Supervisory authorities, recognized accountability agents, trade associations, and government agencies engage in raising the awareness of organisations about the obligations that an accountable organisation must meet, and the benefits that flow from being accountable.

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

Issues for Resolution

1. How will remediation work in an accountability approach?

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

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

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

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

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

2. How do organisations determine the appropriate validation mechanism?

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

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

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

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

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

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

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

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

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

¹⁸ Opinion 3/2010 on the principle of accountability, 13 July 2010, Article 29 Data Protection Working Party, 00062/10/EN, WP 173.

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

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

Conclusion

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

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

- (1) Policies
- (2) Executive oversight
- (3) Staffing and delegation
- (4) Education and awareness
- (5) Ongoing risk assessment and mitigation
- (6) Program risk assessment oversight and validation
- (7) Event management and complaint handling
- (8) Internal enforcement
- (9) Redress

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

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

Appendix

Accountability Project Phase II – The Paris Project Participants

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

Joseph Alhadeff, Oracle Corporation

Amit Ashkenazi, Law Information and Technology Authority, Israel

Carman Baggaley, Office of the Privacy Commissioner, Canada

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Emmanuelle Bartoli, CNIL

Bojana Bellamy, Accenture

Emma Butler, Information Commissioner's Office, United Kingdom

Daniel Burton, Salesforce.com

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

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Leigh Feldman, Bank of America

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Peter Fleischer, Google

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

Christine Frye, Bank of America

Jose Leandro Nunez Garcia, Data Protection Agency, Spain

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

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

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

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Sandy Hughes, Procter & Gamble Company

Peter Hustinx, European Data Protection Supervisor

The Honorable Michael Kirby

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

Laraine Laudati, European Commission

Barbara Lawler, Intuit, Inc.
Artemi Rallo Lombarte, Director, Data Protection Agency, Spain
Brendon Lynch, Microsoft Corporation
Fran Maier, TRUSTe
Olivier Matter, CNIL
Madeleine McLaggan, Commissioner, Data Protection Authority, The Netherlands
Daniel Pradelles, Hewlett-Packard Company
Olivier Proust, Hunton & Williams
Krisztina Rajos, Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary
Kathryn Ratte, United States Federal Trade Commission
Florence Raynal, CNIL
Stéphanie Regnie, CNIL
Sachiko Scheuing, Acxiom
Russell Schrader, Visa Inc.
Manuela Siano, Data Protection Authority, Italy
David Smith, Information Commissioner's Office, United Kingdom
Hugh Stevenson, United States Federal Trade Commission
Blair Stewart, Office of the Privacy Commissioner, New Zealand
Jennifer Stoddart, Privacy Commissioner, Canada
Scott Taylor, Hewlett-Packard Company
Omer Tene, College of Management School of Law, Israel
K. Krasnow Waterman, Massachusetts Institute of Technology
Nigel Waters, Privacy International
Jonathan Weeks, Intel Corporation
Yael Weinman, United States Federal Trade Commission
Boris Wojtan, Accenture

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP
Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP
Richard Thomas, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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

Federal Trade Commission
February 18, 2011

APPENDIX B

Data Tagging for New Information Governance Models

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

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

Although geography and national borders place few inherent limitations on where organizations can transfer data, such boundaries demarcate different and very real requirements and obligations for handling personal information. For owners and processors, moving data across these boundaries presents practical challenges in administering and implementing the rules and laws by which individuals maintain their rights to data protection and privacy. Here, we describe data governance in this complex and dynamic environment, where the rules and obligations that govern how organizations use and protect information attach to the data and must be met wherever or by whomever it is collected, processed, or stored. We can facilitate such an approach via “tagging” data with sufficient information that its recipients and users can understand their specific obligations for its appropriate use and safeguarding.

Approaches to privacy protection that rely exclusively on “notice and choice” have come under significant criticism as being impractical and ineffective. In a notice-and-choice model, consumers receive information about how an organization will collect, use, and share data about them. On the basis of this notification, consumers choose whether to allow its use. Such a model breaks down in an environment in which organizations can analyze and process information instantaneously at the collection point, and where data collection has become so ubiquitous that individuals could receive privacy notices every time they connect to the Web, are monitored by surveillance cameras, use a mobile communications device, or visit a building that uses sensors. In many cases, notices are lengthy and complex, and don’t inform any meaningful choice. Choice itself might now be illusory—at worst, inappropriate, and at best, giving the data custodian or controller helpful parameters for data use only in limited circumstances. Acknowledging this reality, commenters at the FTC “Exploring Privacy” workshops urged policymakers to look beyond notice and choice as the starting point for privacy protection. (For example, in response to the failure of fair information practices, Fred H. Cate argues for a more tailored, re-

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

K. KRASNOW WATERMAN
Massachusetts Institute of Technology

Emerging Approaches to Data Governance

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

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

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

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

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

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

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

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

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

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

Accountability

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

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

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

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

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

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

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

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

Use-and-Obligations Model

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

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

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

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

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

Strategic Information Management

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

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

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

Practical Considerations

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

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

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

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

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

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

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

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

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

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

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

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

References

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

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

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

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