THE BUSINESS FORUM FOR CONSUMER PRIVACY

June 9, 2010

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

Dear Sirs and Madams,

The Business Forum for Consumer Privacy ("the Forum") appreciates this opportunity to respond to the Department of Commerce's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy." The Forum is an organization of companies whose mission is to examine issues related to the next generation of privacy governance in the United States and to propose thoughtful, workable solutions for consideration by experts, businesses and policymakers.[1]

The Forum focuses its response on Question 1 of the Notice of Inquiry. Question 1 references specifically the use-and-obligations model:

> *Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use. Describe how a use-based privacy system would work. How should policymakers determine what constitutes harmful uses of personal information in this model? Are there examples from existing privacy laws and regulations that suggest strengths and weaknesses of the use-based model? Is this "use-based" model for commercial data privacy a workable approach for companies and consumers? What is the relationship between use-based privacy rules and proposed accountability systems?*

As the primary developers of the use-and-obligations model, the Forum will respond to this question by making four points:

1. The nature, speed and volume of data collection, processing and analysis stress legacy models of privacy governance based on traditional models of notice and choice.

---

[1] The Business Forum for Consumer Privacy is an independent project of the Centre for Information Policy Leadership. A list of companies that participate in the Forum's work is attached as Appendix A. Questions related to these comments should be submitted to Martin Abrams at mabrams@hunton.com or to Paula Bruening at pbruening@hunton.com.

2. Obligations related to the way in which data is to be protected and managed must now depend, in many instances, upon the purpose for which the data is to be used.

3. The use-and-obligations model must be adopted and implemented in tandem with an accountability approach to data protection.

1. The nature, speed and volume of data collection, processing and analysis stress legacy models of privacy governance based on traditional models of notice and choice.

Question one of the Notice of Inquiry asks "does the existing privacy framework provide sufficient guidance to the private sector?" The Forum's response is "no."

In February 2010, *The Economist* published a report describing how the revolution in computing and communications technology is changing business processes.[2] The article highlighted the explosion in usable information and the potential it offers if harnessed and used. Coining the term "big data," the report explained the phenomenon of continuous collection, application and reapplication of information. It noted the capacity of big data to both promote innovation and raise significant privacy concerns.

Legacy privacy governance systems date to the early 1970s when single-application mainframe systems were the norm and data resided on punch cards. Governance was designed to facilitate the ability of individuals to control the flow of data about themselves, and relied upon notice of data collection, use and sharing, and individual choice based on that notice at the point of data collection. Organizations are obligated to use and protect data based on that choice.

Today data is collected through keystroke monitoring and by observing how long a mouse hovers over an image. Information is gathered through geo-location devices and sensor-based technologies. Data is collated and analyzed in real time to facilitate targeted advertising and optimize the online experience. Information may be processed in the facility near corporate headquarters, or in a data warehouse halfway around the globe. In the age of big data, the complexity of data collected and used and the time necessary for consumers to make informed decisions based on notices test the current model of governance.

[2] "Data, data everywhere: A special report on managing information," *The Economist*, February 27, 2010.

2. Obligations related to the way in which data is to be used and protected must now depend, in most instances, upon the purpose for which data is to be used. The use-and-obligations model provides such an approach.

When the Forum began its exploration of new approaches to privacy governance, it assumed traditional notions about data: that it is or is not sensitive; that it is personally identifiable or it is not; and that uses of data fall into two categories — primary and secondary. In testing governance approaches based on these assumptions, it quickly became clear that in the current environment of data collection, analysis, storage and processing, these commonly accepted distinctions did not facilitate effective protection. The Forum looked instead to a model that turns on distinctions about the *use* of the data, rather than about the data itself.

The use-and-obligations model, explained in depth in the Forum's release " A Use-and-Obligations Approach to Protecting Privacy: A Discussion Document,"[3] has the following characteristics:

- The use-and-obligations model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment and management of the relationship with the consumer; 2) internal business operations; 3) marketing; 4) fraud prevention and authentication; and 5) external, national security and legal processes.[4]

- The use-and-obligations model does not attempt to preclude principles of fair information practices, nor to take the place of applicable law.[5] Rather, it proposes a method to implement those principles in a way that reflects current technology, business processes and data use.

- The use-and-obligations model recognizes two aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organizations must

[3] Released December 7, 2009, attached as Appendix B, and found at http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf (last visited June 3, 2010).

[4] While the Forum identified these five categories, there may be more. The obligations related to additional categories of use, once identified, must be tested and vetted.

[5] In particular, laws and self-regulatory codes should continue to protect individuals from the deceptive and fraudulent collection of information. Possession of data should continue to trigger security requirements. The use-and-obligations model depends on these regulatory protections.

take to facilitate individual participation: transparency (notice), choice[6], and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and appropriate; and can access and correct it in appropriate circumstances. The second aspect includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual: collection limitation and data use minimization; data quality and integrity; data retention; security; and accountability.

- The use-and-obligations model encourages trusted data protection by requiring that the obligations that attach to data — whether from law, industry guidance or the organization's promises — should remain with the data and be met wherever or by whomever it is processed.

3. The use-and-obligations model should be adopted and implemented in tandem with an accountability approach to data protection.

In an environment of rapid data sharing, business process outsourcing and use of vendors to provide services, a use-and-obligations model can work effectively only if the obligations that arise with respect to the use of data are honored no matter where the data is transferred, stored or processed. Therefore, for the use-and-obligations model to succeed, all organizations that use data must be accountable — they must be able to demonstrate their ability to honor the obligations that come with the data, and to understand and mitigate risks to individuals raised by the data's sharing and use.

Accountability is a well-established principle of data protection, found in known guidance such as the OECD Guidelines; in the laws of the European Union, the EU member states, Canada and the United States; and in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. Recently, participants in an international working group facilitated by the Centre for Information Policy Leadership[7] defined in specific terms what it means for organizations to be accountable.

---

[6] The use-and-obligations model enhances the fair information practice of transparency, by requiring transparency and choice based on the nature of the data use. Organizations would be required to provide "just-in-time" notice when the individual would not expect the data use.

[7] Participants in the work included representatives of privacy enforcement agencies, governments, civil society and the private sector. The results of the first year's meetings in Ireland are found in "Data Protection Accountability: The Essential Elements," October 2009, attached as Appendix C, and found at http://www.huntonfiles.com/files/ebupload/CIPL_Galway_Accountability_Paper.pdf (last visited June 3, 2010).

The essential elements of accountability are:

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

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

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

4. Transparency and mechanisms for individual participation.

5. Means for remediation and external enforcement.

Accountability provides an infrastructure for the use-and-obligations model that encourages organizations to engage in the risk assessment and mitigation necessary to meet obligations appropriately. It also creates a culture of privacy such that companies transferring data for processing and those receiving it do so with an understanding of what will be required to use data responsibly.

Conclusion

The Forum does not view the use-and-obligations model as a legislative framework, but rather offers it as an example of a governance approach that is workable in the current digital economy. The Forum has tested the model across various industry sectors, technologies and data applications, and has found it to consistently offer practical guidance. The model is adaptable where there is omnibus privacy law, and where industry sectors (*e.g.*, health care and finance) impose specific requirements.

The Forum is encouraged by the Department of Commerce's return to its traditional leadership role in encouraging privacy and innovation in the digital economy. We believe that the use-and-obligations model has promise, but acknowledge the significant additional work that must be carried out before it might be proposed as part of a governance package. We look forward to working with the Department of Commerce as it continues to explore this approach.

Yours sincerely,

/s/

The Business Forum for Consumer Privacy

APPENDIX A

THE BUSINESS FORUM FOR CONSUMER PRIVACY

List of Member Companies

AT&T
eBay, Inc.
Google
Hewlett-Packard
Intel
Intuit
Microsoft
Oracle
Procter & Gamble
Wal-Mart

APPENDIX B

A USE AND OBLIGATIONS APPROACH TO PROTECTING PRIVACY: A DISCUSSION DOCUMENT

The Business Forum for Consumer Privacy

December 7, 2009

Introduction

This paper proposes a framework for implementation and interpretation of traditional principles of fair information practices that reflects and serves the way data is used and managed in the 21st century.

Principles of fair information practices continue to form the foundation for effective, reliable privacy and data management and protection. They provide for transparency around the collection and use of data; engagement of the individual in decisions about how data pertaining to them may be used; data security; and protections to ensure that decisions about the consumer are based on data of appropriate quality. While principles of fair information practices remain relevant to sound data protection today, our traditional way of applying those principles may not effectively provide consumers with adequate protection.

First articulated in 1973,[1] fair information practices were developed to establish ways in which individuals might exercise control over personal information. The principles provide that individuals are given notice about how their data will be used. Based on that notice, individuals either consent to or prohibit its use. Organizations specify the purposes for which data is collected and limit collection to the data that is needed. In appropriate circumstances, individuals are granted access to data pertaining to them. Organizations are required to secure the data they collect to ensure its integrity and availability, and are held accountable for the manner in which their data management reflects principles of fair information practices.

The principles are widely endorsed and adopted. They form the basis of recognized guidance promulgated by the Organization for Economic Cooperation and Development, Asia Pacific Economic Cooperation, and the United States Federal Trade Commission. They are reflected in the European Union Privacy Directive, federal and state/provincial laws in many countries, self-regulatory regimes, and industry codes of conduct. Principles of fair information practices serve as the starting point for privacy protection around the world.

These practices continue to serve the privacy interests of individuals and the needs of business. They have proven dynamic enough to address privacy through a period of rapid and dramatic evolution in data use and technology innovation. But the realities of a data-fueled economy require a re-examination of how to implement the principles in a way that most effectively serves the consumer.

As currently implemented, fair information practices enable the consumer to read a privacy notice and make choices, to the extent they are available, based on what he understands of that notice. The collecting organization promises not to use data in a manner that is not consistent with the consumer's choice.

But today, online and in public life, individuals, organizations and data analytics generate ever-growing amounts of data that fuel existing and emerging business processes. Wireless and mobile communications offer new points of data collection and provide new kinds of data. Open networks and the evolution of the Internet as a commercial medium and as a platform for connected services enable ubiquitous collection and global flow of data. Data about an individual can be easily copied and aggregated across vast, interconnected networks. That data, enhanced by analytics, yields insights and inferences about individuals based on data maintained in multiple databases scattered around the world. Asking the individual to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it provide a sufficient check against inappropriate and irresponsible data use in the marketplace.

In this paper, the Business Forum for Consumer Privacy[2] (BFCP) proposes a *Use-and-Obligations* model — a framework for implementation and interpretation of traditional principles of fair information practices in a manner that reflects and serves

1 "Records, Computers and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health Education and Welfare, 1973.

2 The Business Forum for Consumer Privacy (BFCP) sponsors this paper. The BFCP has taken up the work of the Consumer Privacy Legislative Forum to explore new privacy governance frameworks. The consensus of the BFCP is that the United States' current, often conflicting, mix of sector specific laws at both the federal and state level creates inefficiencies for businesses and often denies appropriate protections for consumers. The BFCP is dedicated to creating new frameworks that will be the basis for privacy governance as reflected in company best practices, industry codes and workable new or revised laws where necessary with a principle focus on the US marketplace.

the way data is used and managed in the 21st century. While the collection of data and consumer consent to — or choice about — its use traditionally have triggered an organization's obligations to protect data, this paper proposes an approach in which *the way an organization **uses** data determines the steps it is **obligated** to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use.*

This proposed Use-and-Obligations model in no way attempts to preclude principles of fair information practices, nor to take the place of applicable law. Rather, it proposes a practical, contemporary means to implement those principles, in the context of business processes and data uses enabled by 21st century technology, and supplements them with additional protections.

Overview of the Use-and-Obligations Approach

The Use-and-Obligations model establishes the use rather than the collection of data as the primary driver of a data collector's obligations related to notice, choice, and access and correction. Under current implementation of fair information practices, consumer choice or consent to use data in certain ways establishes a company's responsibilities. A Use-and-Obligations model shifts responsibility for disciplined data use to the data collector and all holders (e.g. third party vendors) of data, imposing requirements for transparency and notice, consumer choice, and access and correction on the data collector based upon the way the data is to be used.

The model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment, 2) internal business operations, 3) marketing, 4) fraud prevention and authentication, and 5) external, national security and legal.[3]

The Use-and-Obligations model recognizes two aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organizations must take to facilitate individual participation — transparency (notice), choice, and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and appropriate; and can access and correct it in appropriate circumstances. The second aspect includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual — collection limitation and data use minimization; data quality and integrity; data retention; security; and accountability. The uses and obligations are discussed below.

Categories of Use

Fulfillment. Fulfillment includes the activities necessary to establish and maintain the relationship between the organization and the consumer. It includes activities related to the purchase, payment for, and delivery of a product or service. Fulfillment also involves ongoing customer service and support. Fulfillment triggers data uses that are normally expected or explicitly consented to by the consumer. It requires high-quality data, because the decisions based on that data can have significant consequences.

Internal Business Processes. Internal business processes include activities necessary to operate a business, such as accounting; audit and compliance; staff scheduling; management of information technology infrastructure; and product and service development, improvement, and testing. All require data related to customers, but processing primarily involves the internal functioning of the business.

3 While the BFCP has identified these five categories, there may be more. The obligations related to those additional categories of use, once identified, must be tested and vetted.

Marketing. Marketing includes activity related to making offers to existing customers and personalizing products or services at their request, targeting individuals as potential customers, developing a strategy to reach those customers, determining the prices and terms to be offered, and selling or upgrading products and services.

Fraud Prevention and Authentication. Organizations use personal information to prevent fraud, identify individuals, authenticate that they are who they say they are, verify that they may act in certain ways (e.g., to access their data or to engage in an online activity, such as banking or account management), and establish their eligibility for benefits or services. Some of the data necessary to perform these functions may come directly from the individual and some may come from third-party services, such as credit reporting agencies.

National Security and Legal. Government and law enforcement agencies may approach organizations with a subpoena or court order to obtain data pertaining to an individual. U.S. courts may grant fairly broad discovery rights to parties in legal proceedings. These uses are often beyond the control of the organization that collect or store the data.[4]

Categories of Obligations

The obligations incurred by organizations fall into two categories: those that facilitate the individual's participation and those that involve an organization's internal activities to assess and mitigate risks to individuals raised by data collection and use.

I. Facilitating Individual Participation

Transparency/Notice. Transparency involves notifying the individual about the collection and use of data. The posted notice of a company's privacy policy is the foundation of transparency. The Use-and-Obligations model references two kinds of notice to ensure transparency — *discoverable notice* and *just-in-time notice.*

Discoverable notice is a posted notice of an organization's privacy policy that can be easily located and accessed by the consumer. Discoverable notice may take the form of, for example, the notices required by the Gramm-Leach-Bliley Act and sent to consumers by U.S. mail, notices posted on a website, notices made available in a health care provider's office according to the provisions of the Health Information Portability and Accountability Act, and notices made available on paper at a point of purchase in a retail establishment.

For purposes of this analysis, just-in-time notice generally is provided when uses of data likely are not to be expected by the individual.[5] It generally appears or is made available at the point where a consumer is required to make a decision about entering into a transaction or about the use or sharing of data for a specific purpose or set of purposes.

Choice. In some cases, individuals may have a choice about the use of their data. That choice may be offered as an opt-in (the individual affirmatively requests that data be used in a certain way) or as an opt-out (the data collector assumes that data can be used in a certain way unless the individual indicates otherwise; the individual is offered a clearly conspicuous, easily accessible way to decline the use of his data). In some cases, the individual practically may not be able to exercise choice. For example, in order to have merchandise sent to his home, the individual must allow that his data be used for shipping. In other cases, such as direct postal marketing, the consumer may have a choice.

Access and Correction. Access and correction serve two purposes. First, they facilitate transparency and individual participation by informing individuals about what kind of data about them an organization maintains and stores. Second, they promote the accuracy and quality of data and the suitability for a specific purpose.

---

4 Organizations that collect and process data in general take national security and legal requirements seriously and take steps to respond to them appropriately. However, an organization's inability to ensure that obligations related to data are respected once that data is shared with government may compromise the effectiveness of the Use-and-Obligations model. The BFCP believes that issues related to the accountable use of data by government should be publicly discussed and addressed. They are not, however, the subject of this paper.

5 Questions related to when and how practically to provide effective just-in-time notice remain the subject of discussion, and are beyond the scope of this paper.

The Use-and Obligations model provides for two kinds of access. To facilitate transparency, it provides for what is referred to as *generalized* access. Generalized access involves providing the individual with the categories of data the organization holds about the individual (or type of individual), but does not require the organization to provide the consumer with the data itself.

To ensure the accuracy, usability, and sufficient quality of the data, the Use-and-Obligations model also provides for access to the specific data maintained about the individual, and an opportunity to challenge and, where appropriate, to correct the data.

II. Internal Assessment and Mitigation of Risk

Collection Limitation. Collection limitation requires that organizations only collect data for which it has a use or purpose. In general, organizations typically identify three uses — prevention of fraud, fulfillment, and marketing. Collection limitation mitigates the risk of data breach, as the more data an organization holds, the greater the potential risks to the individuals and the more effort the organization must undertake to protect it. Collection limitation can prompt an organization to manage risk through more strategic and thoughtful plans for data collection and use.

Data Use Minimization. While not explicitly stated in traditional expressions of fair information practices, data use minimization is included in this discussion because it functions as an adjunct to collection limitation, and reflects the orientation and application of fair information practices toward use, rather than collection, of data. Data use minimization, along with collection limitation, requires that organizations determine what data should be used to provide for the optimal function of a business process, product or service, and then use only that data. Data use minimization prompts an organization to more thoughtfully and strategically reduce the risk of exposure or breach of an individual's data that might result from the improper actions of parties internal or external to the organization.

Data Quality/Integrity. Data quality and integrity requires that organizations use data whose quality is suited to the use to which it is put, and that data is usable when needed to facilitate business process or deliver products or services requested by the consumer. Data quality requirements depend on the data's sensitivity, the degree of accuracy required, the nature of the use, and the risk to individuals of inaccurate results.

Data Retention. Data retention provides that organizations retain data only as long as it is of some use to the organization or the individual. Data retention protects the individual against the risk raised by use of antiquated data that no longer reflects and individual's current circumstances

Security. Organizations have an affirmative obligation to keep data safe from compromise, improper use, and breach.

Accountability. An organization must be responsible and answerable for its actions related to all obligations in a Use-and-Obligations model.

Prevention of Harm

Prevention of harm to individuals through appropriate risk and data management practices serves as both the motivation for meeting these obligations and as the metric by which their successful fulfillment is evaluated.[6] Users of data must consider the risk to individuals to whom the data pertains, and take steps to prevent harm that might result from the use of the data. The concept of harm can include, among other things, compromise of an individual's financial or physical well-being, embarrassment, and damage to reputation.[7]

6 The APEC Privacy Framework sets out prevention of harm as its first principle.
7 Additional work is needed to more clearly define and describe harm, as it can result from violation of privacy and inappropriate use of data.

The Use-and-Obligations Analysis — Table A

Table A offers a visual analysis of the Use-and-Obligations model. This section walks the reader through an analysis of each category of data use and the obligations triggered by that use. Part I of the analysis first examines the obligations related to individual participation. Part II reviews the internal risk assessment and mitigation obligations.

Table A
Use and Obligations Approach

	Use Categories		Fulfillment (Establish& Maintain Relationship)	Internal Business Processes	Marketing	Fraud Prevention & Authen-tication	National Security & Legal
Part I -- Individual Participation	Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
		Just-in-time Notice	No	No	For any Unexpected Uses	No	--
	Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
		Access	Yes	--	Generalized Access: Summary of Data Collected	Limited with Authentication	--
		Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Part II -- Internal Risks	Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
		Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
		Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
	Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
	Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
	Accountability						As Required by Law
	Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

I. Facilitating Individual Participation

Fulfillment

Transparency/Notice. Consumers must be provided a discoverable notice about data collection and uses for transaction fulfillment and service delivery. Just-in-time notice is not required, although consumers may appreciate such a notice for certain complex transactions or services.

Choice. The organization must use data necessary for fulfillment to complete the transaction or deliver the service to the consumer. For example, in the case of fulfillment of a transaction, the consumer has no explicit choice about this data use; if the company cannot collect this data, it cannot fulfill the transaction and the relationship between the company and the consumer effectively ends. In the case of delivering a service, the consumer has made an implicit choice about data use by subscribing to the service.[8]

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish & Maintain Relationship)	Internal Operations	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	--
Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
	Access	Yes	--	Summary Of Data Collected	Limited with Authentication	--
	Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

Access and Correction. Fulfillment data makes it possible for the organization to deliver a service to the customer. It also provides the basis for decisions related to the customer's ability to purchase goods or services, or to where goods or services are delivered. Fulfillment data, therefore, must be accurate and current. The consumer's ability to access his data and correct any errors is necessary to ensure its integrity. Companies are, therefore, obligated to provide consumers with the ability to access and correct data.

Internal Business Processes

Transparency/Notice. Consumers must be given notice of data use for internal business processes. Just-in-time notice is not required, because consumers would not find the uses unexpected.

Choice. The consumer is not given a choice about the use of data for business operations, because this use is necessary to basic business functions such as accounting and internal auditing.

Access and Correction. Organizations are not required to provide access and correction because the data used for internal business processes is generated through the fulfillment process. As noted, the Use-and-Obligations model provides for access and correction to this data for its use in fulfillment.

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish & Maintain Relationship)	Internal Operations	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	--
Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
	Access	Yes	--	Summary Of Data Collected	Limited with Authentication	--
	Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

Marketing

Transparency/Notice. Just-in-time notice must be provided if the marketing initiatives would not be expected by the consumer. For other marketing, companies must provide an easy-to-read, discoverable privacy policy.

Choice. At a minimum, the consumer must be offered the opportunity to opt out of marketing.

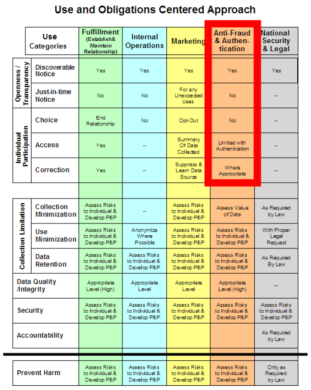
Access and Correction. Consumers must, upon request, be provided generalized access — a summary of the kinds of data used for marketing. As marketing data does not form the basis for critical decisions about the individual, access to specific data is optional but not required.

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish & Maintain Relationship)	Internal Operation	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	--
Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
	Access	Yes	--	Summary Of Data Collected	Limited with Authentication	--
	Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

8 In some instances, the organization may be able — and may choose — to fulfill a transaction or continue to provide the service even when the customer has chosen not to have data used for this purpose.

Fraud Prevention and Authentication



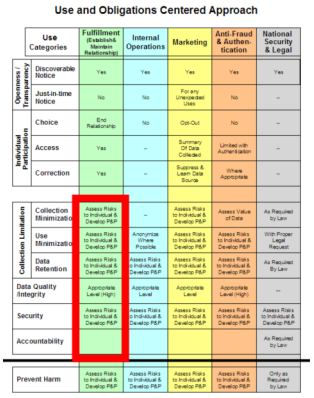
Transparency/Notice. Just-in-time notice is not required. However, the privacy policy must state that the data is used to prevent fraud.

Choice. Consumers have no choice about these uses, for reasons of public policy, safety and security.

Access and Correction. Limited access to data that will not compromise fraud analysis and authentication functions is provided, so that individuals can understand what data about them is being processed.

II. Risk Assessment and Mitigation

Fulfillment



Collection Limitation. Organizations must assess what data they reasonably need to complete a transaction with a consumer and deliver goods or services. It must also consider what data may be required to provide ongoing service delivery or extended service, if appropriate, and to fulfill warranty requirements. It should assess any risks related to storage of that data and address them as necessary.

Use Minimization. Once collected, organizations must determine who needs to see the data, and under what conditions or circumstances. They must also decide for what other business functions besides fulfillment the data must be accessible. Use minimization involves limiting the amount and kind of data used in a specified business process, product, or service to that needed to achieve identified goals.

Data Retention. Organizations must assess risks to individuals raised by retaining data, develop practices and procedures to determine when it is no longer useful, and develop schedules and procedures for appropriately retiring the data.

Data Quality and Integrity. Data related to fulfillment usually includes, among other things, name, address, and credit card data. Because it is important both to the organization and the individual that fulfillment data be correct, data quality requires that the organization ensure that the data be complete, current, and accurate.

Data Security. Organizations must assess risks to individuals raised by the capture, storage, and processing of fulfillment data and develop security policies and procedures to effectively manage those risks.[9]

Accountability. Organizations must have in place policies, procedures, training, and compliance assessment to ensure that use of data for fulfillment is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

9 Organizations must also assess and manage security risks related to processing of data by business partners.

Internal Operations

Collection Limitation. Organizations must anticipate what data they will reasonably need to carry out internal functions such as accounting; marketing research and trend analysis; product analysis, improvement and development; commissions; and performance evaluations. Based on that assessment, they must collect only that data necessary to perform those internal functions.

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish& Maintain Relationship)	Internal Operations	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	--
Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
	Access	Yes	--	Summary Of Data Collected	Limited with Authentication	--
	Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

Use Minimization. Once collected, organizations must determine who needs to view or access the data for internal operations under what conditions or circumstances, and limit its use accordingly. They must also decide to which other business functions in an organization the data must be accessible and for what purposes. Use minimization also involves limiting the amount and kind of data used in a specified business process, product, or service only to that needed to achieve identified goals.

Data Retention. Organizations must determine how long data is needed, and assess the risks to individuals raised by retaining data. In light of that assessment, organizations should develop a schedules, policies, and procedures for retiring the data.

Data Quality and Integrity. Data used for internal operations can influence decisions related to budget planning, employee compensation, and commissions. Organizations must ensure that the quality of the data is at a level appropriate to its intended use.

Data Security. Organizations must assess risks to individuals raised by the capture, storage, and processing of data and develop security policies and procedures to effectively manage those risks.

Accountability. Organizations must have the policies, procedures, training, compliance assessment, and oversight in place to ensure that data is used for internal purposes in accordance with the organization's agreed-upon decisions.

Marketing

Collection Limitation. Organizations collecting and using data for marketing purposes must consider what data they legitimately need for marketing, and the risks related to storing additional data collected from consumers and third parties. They are required to consider the sensitivity of the data and the costs to secure it in light of its usefulness and predictive value. Based on that analysis, organizations must develop policies and practices to address risks raised by the data they choose to collect and retain for marketing.

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish& Maintain Relationship)	Internal Operations	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	--
Individual Participation	Choice	End Relationship	No	Opt-Out	No	--
	Access	Yes	--	Summary Of Data Collected	Limited with Authentication	--
	Correction	Yes	--	Suppress & Learn Data Source	Where Appropriate	--
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	--	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality /Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	--
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

Use Minimization. Data may vary in its ability to identify consumer preferences and predict consumer buying behavior. Use minimization requires that organizations use in marketing applications only data that is effective and yields useful results. Use minimization enhances overall data security by reducing risk of data exposure and loss.

Data Retention. Organizations must assess the risks that retaining data raises for individuals, develop practices and procedures to determine when it is no longer useful, and establish schedules and procedures for appropriately retiring it.

Data Quality and Integrity. In analyzing data for potential use in marketing, organizations must consider — among other things — whether it can be used lawfully, whether its use is governed by contractual obligations, and whether permissions related to data must be respected. Organizations must determine whether data is sufficiently predictive to be suitable for marketing.

Data Security. Organizations must assess risks to individuals raised by the capture, storage and processing of data and develop security policies and procedures to effectively manage those risks.

Accountability. Organizations must have in place policies, procedures, training, and compliance assessment to ensure that use of data for marketing is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

Fraud Prevention and Authentication

Collection Limitation. Data required for fraud prevention and authentication — such as log-in credentials, social security number, mother's maiden name, account data, patterns of account activity — can be especially sensitive. The principle of collection limitation provides that only data necessary to carry out these functions be collected.

Use Minimization. Because fraud prevention and authentication data is sensitive, organizations must take particular care to ensure that only the data necessary is used to perform desired functions. In many cases, the results of fraud analysis and authentication proofing may be provided to an organization's personnel who will need only the results of this activity. In such cases, personnel will have limited — if any — access to the raw data on which it is based.

Use and Obligations Centered Approach

	Use Categories	Fulfillment (Establish & Maintain Relationship)	Internal Operations	Marketing	Anti-Fraud & Authen-tication	National Security & Legal
Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
	Just-in-time Notice	No	No	For any Unexpected Uses	No	–
Individual Participation	Choice	End Relationship	No	Opt-Out	No	–
	Access	Yes	–	Summary Of Data Collected	Limited with Authentication	–
	Correction	Yes	–	Suppress & Learn Data Source	Where Appropriate	–
Collection Limitation	Collection Minimization	Assess Risks to Individual & Develop P&P	–	Assess Risks to Individual & Develop P&P	Assess Value of Data	As Required by Law
	Use Minimization	Assess Risks to Individual & Develop P&P	Anonymize Where Possible	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	With Proper Legal Request
	Data Retention	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	As Required By Law
Data Quality Integrity		Appropriate Level (High)	Appropriate Level	Appropriate Level	Appropriate Level (High)	–
Security		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P
Accountability						As Required by Law
Prevent Harm		Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Assess Risks to Individual & Develop P&P	Only as Required by Law

Data Retention. Organizations must determine for how long they must keep data to protect the organization from legal challenges, and assess the risks that retaining data raises for individuals. Based on that analysis, they must develop practices and procedures to determine when data is no longer useful, and develop schedules and procedures for appropriately retiring it.

Data Quality and Integrity. Fraud prevention generally requires use of data of sufficiently high quality to reliably identify bad actors and avoid false positives. Authentication requires accurate and current data to assess whether an individual is who he says he is, and verify that he is authorized to engage in certain activities or to access physical places, accounts, records, or data.

Data Security. Organizations must assess the risks that the capture, storage and processing of data raises for individuals, and develop security policies and procedures to address those risks. Data used for authentication purposes may be particularly sensitive because it can identify individuals and allow access to accounts and data. Fraud data, especially data that identifies a person as one who might possibly perpetrate fraud, also raises risks to reputation and to an individual's ability to engage in transactions or obtain financial services. Security for such data should be enhanced.

Accountability. Organizations must have in place policies, training and procedures to ensure that data used for fraud prevention is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

The Use-and-Obligations Approach: The Hotel Example — Table B

A stay at a hotel provides a practical example of how principles of fair information practices would be implemented according to a Use-and-Obligations model. It also illustrates the way in which data about a hotel guest flows between organizations to deliver the full range of hospitality services involved in a hotel stay. It further demonstrates how a Use-and-Obligations model would facilitate application of fair information practices as data is shared across entities.

An individual who books a reservation with a hotel engages with a complex network of entities that provide services for a guest's stay and develop a relationship with the guest so that future visits can be best tailored to his preferences. The chain (e.g., Hilton, Marriott, or Inter-Continental), the hotel (the individual physical property), the restaurant, the Internet provider, and the television and radio entertainment services delivered in the sleeping rooms are each owned and operated by discrete,

independent entities. All of these entities collect data from the guest and share that data with the hotel to provide services to the guest and to facilitate basic processes like billing and distribution of revenue to the appropriate service provider.

The guest may book his reservation through the chain's website or 800 number. The reservation is sent to the hotel with contact data, preferences, and any data the guest may have provided through the chain's loyalty program. When the guest registers at the hotel, the registration desk confirms the data and may collect additional data. At registration the hotel becomes the primary manager of the guest's data for the duration of the stay.

During the hotel stay, the guest may avail himself of various services — he may buy a book in the gift shop, dine in the restaurant, and rent movies on the entertainment system.[10] While independent entities provide each of these services, each shares data with the hotel so that fees can be charged against the guest's master bill.

Fulfillment

The hotel collects data that it needs to book a reservation, collect payment and ensure that the guest's stay meets expectations. Fulfillment data may include preferences for furnishings in the room (bed size, pillow type, smoking/non-smoking). It may also include data about diet preferences and location of the room in the building. At the time the reservation is booked, the chain may provide the hotel with additional data derived from the guest's participation in the chain's loyalty program. To ensure payment, service providers share billing and data about charges for services with the hotel. To maintain the relationship with the consumer, the hotel shares with the chain any changes in preferences the guest may indicate during his stay.

Transparency/Notice. The privacy notice posted on the hotel chain's website describes the nature of the data collected by the hotel and the way it is used.

Choice. Because the data is used to complete the transaction with the consumer, there is no choice about its collection and use.

Access and Correction. The consumer is granted access and the ability to challenge — and when appropriate — correct data for fulfillment.

Collection Limitation. The chain and the hotel must determine how much data it needs to deliver the service expected and limit its data collection accordingly.

Use Minimization. The hotel must take steps to ensure that appropriate personnel within the hotel have only the data they need to meet their job requirements. For example, the desk clerk may only need basic identification and payment data, while housekeeping may require data about pillow and temperature preferences but have no need for credit card data. Data may also be shared with independent service providers operating within the hotel. Use limitation ensures that data is available only to the appropriate parties within an organization or to its service providers or partners. Video services may share the fact and frequency of a guest's use of video services for billing purposes, but not the titles of specific movies or the nature of their viewing preferences.

Data Retention. The hotel must make decisions about how long fulfillment data reasonably can be expected to be useful, and develop schedules and protocols for its destruction or retirement when appropriate. Maintaining data beyond its usefulness raises security risks of loss, misappropriation and misuse.

10 The data collected, used, and shared by the entertainment service provides an interesting example. The entertainment company can ascertain only the room occupied by the guest, the dates stayed and the services purchased. None of that data is collected or stored by the entertainment service in a way that is personally identifiable. The entertainment service sends data back to the hotel to facilitate billing. That data includes the names of the movies the guest viewed, when he viewed them, and the fee for each. Because the hotel can link that data to the guest's name, it is stored as personally identifiable by the hotel.

Data Quality and Accuracy. The hotel must take reasonable steps to ensure that fulfillment data is complete, current and accurate.

Data Security. As fulfillment data may contain sensitive data such as credit card numbers, it is important that it be appropriately secured to mitigate the risks to the hotel customer.

Accountability. The hotel must have in place policies, training and procedures to ensure that use of data for fulfillment purposes is managed in accordance with agreed-upon decisions. The hotel is answerable for that management.

Internal Business Processes

The chain and the hotel retain the guest's registration and a record of all purchases and transactions that take place during the stay in order to troubleshoot, maintain quality, improve processes, and conduct surveys.

Transparency/Notice. The chain and the hotel are required to disclose the nature of the use of customer data for internal business processes. Just-in-time notice is not required because these uses are expected.

Choice. The hotel does not give the guest a choice about the use of data for business operations, as such uses are necessary to normal business practices such as accounting and internal auditing.

Access and Correction. Neither the chain nor the hotel is required to provide access and correction because this data is generated through the fulfillment process. As noted, the Use-and-Obligations model provides for access and correction to this data for its use in fulfillment.

Collection Limitation. Data used for internal business purposes is derived primarily from fulfillment data. Data is not collected specifically to facilitate internal business processes.

Use Minimization. To minimize exposure to risk of loss or of internal or external misuse, the hotel must use only that data necessary to support internal functions.

Data Retention. The hotel should retain data only for as long as it is useful for internal business operations.

Data Quality and Integrity. As data is critical to the hotel's ability to deliver its service and receive payment, the hotel must take reasonable steps to ensure that fulfillment data is complete, current and accurate.

Data Security. Data used for these purposes should be secured in a manner commensurate with its sensitivity and the nature of its use.

Accountability. The hotel must have in place policies, training, and procedures to ensure that use of data for internal business processes is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

Marketing

Both the chain and the hotel use data collected from reservations and records of guest stays as a means to market to consumers.

Transparency/Notice. The hotel must provide a discoverable privacy policy that describes the way in which the hotel uses data. The hotel must provide just-in-time notice if it intends to use the data for some unexpected marketing purpose.

Choice. The consumer may opt out of the use of data for marketing at the time of registration and on the website.

Access and Correction. The consumer has the right to generalized access — a summary of the type of information that is used for marketing, and to opt out of its use for this purpose. In this instance, the data comes directly from the fulfillment process and is therefore directly available to the consumer.

Collection Limitation. Because fulfillment data is used for marketing, decisions about collection limitation are conducted in that context. The hotel collects any data needed for internal business processes from the consumer at the time of booking or reservation.

Use Minimization. The hotel must assess data to determine whether it is necessary and appropriate for marketing purposes. The hotel must decide what data collected for fulfillment is used for marketing. For example, the hotel may decide that data about the use of in-room entertainment that is collected for fulfillment (and internal business processes) should not be used for marketing, because such data may raise privacy risks for the consumer. However, data about the guest's frequent use of spa services helps the hotel identify customers interested in such services and poses minimal risk to privacy.

Data Retention. The hotel should develop and implement a policy for determining when data is no longer needed for marketing purposes and for its disposal.

Data Quality and Accuracy. Any third-party data for marketing purposes must be assessed to determine that it is accurate enough to be used for marketing and can be managed to mitigate any risk to privacy.

Data Security. The hotel should secure marketing data in a manner commensurate with its sensitivity and the risk that its loss raises for hotel customers.

Accountability. The hotel must have in place policies, training, and procedures to ensure that use of data for marketing is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

Fraud Prevention and Authentication

The hotel uses data to support fraud probability analysis and to enable authentication proofing. Third parties conduct most of that analysis. The hotel staff inspects identification documents (e.g., passport, drivers license) at check-in, but does not retain identification data.

Transparency/Notice. The hotel privacy policy must indicate that data is used for anti-fraud analysis and authentication. Just-in-time notice is not required.

Choice. Individuals have no choice about use of data for these purposes, for reasons of public policy, safety and security.

Access and Correction. The hotel is required to provide limited access to data that will not compromise fraud analysis and authentication functions, so that individuals can understand what data about them is being processed for these purposes.

Collection Limitation. The hotel likely uses an outside vendor to provide fraud prevention and authentication services. The hotel will be required to collect data deemed necessary by the service to support its analysis.

Use Minimization. Data about fraud prevention and authentication will only be shared within the organization on an as-needed basis. Hotel clerks, for example, will need only the results of fraud probability analysis and the "yes" or "no" answer to identity authentication. The clerk does not need to see the raw data used to provide those results.

Data Retention. Because the data required for fraud prevention and authentication is sensitive, its retention can raise risks to the hotel customer. The hotel should retain the data for as along as necessary to protect the hotel: to validate or justify its findings, to fulfill legal requirements, or to rebut challenges. The data should be disposed of when it is no longer useful for these purposes.

Data Quality and Integrity. Because of the potential consequences for the consumer, it is critical that the data analyzed for prevention of fraud and authentication be of a quality necessary to yield accurate results. The hotel must ensure that the service provider it enlists for these services has sufficiently accurate, current, and complete data to serve these purposes.

Data Security. The hotel should secure the data analyzed for fraud prevention and authentication proofing in a manner commensurate with its sensitivity and the risk of its loss raises for hotel customers.

Accountability. The hotel must have in place policies, training, and procedures to ensure that use of data for fraud prevention and authentication is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

Hotel Use and Obligation Chart

Table B
Hotel Example

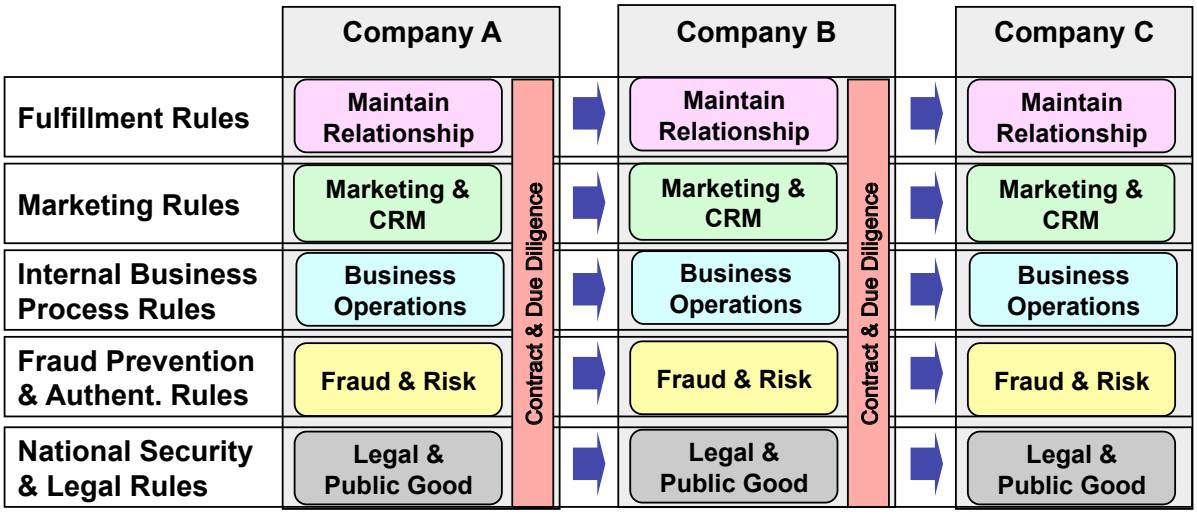
		Use Categories	Fulfillment (Establish& Maintain Relationship)	Internal Business Processes	Marketing	Fraud Prevention & Authen-tication	National Security & Legal
Part I -- Individual Participation	Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
		Just-in-time Notice	No	No	No	No	N/A
	Individual Participation	Choice	Yes	No	Yes	No	N/A
		Access	Yes	No	Generalized Access: Summary of Data Collected	No	N/A
		Correction	Yes	No	Opt-Out	No	N/A
Part II -- Internal Risks	Collection Limitation	Collection Minimization	Yes	There is no specific collection for this use	Only necessary for marketing	All data necessary to prevent fraud	As required by law
		Use Minimization	Yes	Only use data necessary	Only necessary for marketing	All data necessary to prevent fraud	Only what required
		Data Retention	For period necessary	For period necessary	For period necessary	For period necessary	As required by law
	Data Quality /Integrity		Must be very accurate	Appropriate Level	Appropriate Level	Must be very accurate	N/A
	Security		Appropriate for payment information	Appropriate for payment information	Appropriate for data used	Appropriate for sensitivity of the data	Data conveyed in a secure fashion
	Accountability		Appropriate policies and procedures to mitigate risks	Appropriate policies and procedures to mitigate risks	Appropriate policies and procedures to mitigate risks	Appropriate policies and procedures to mitigate risks	Appropriate policies and procedures to mitigate risks
	Prevent Harm		Assess risks to individual & develop policies and procedures	Assess risks to individual & develop policies and procedures	Assess risks to individual & develop policies and procedures	Assess risks to individual & develop policies and procedures	Only as required by law

Data Flow Among Affiliated Companies — Table C

In an information-based economy, data flows from organization to organization to facilitate fulfillment of orders and delivery of products and services; to provide customer care; to invoice customers; and to deliver advertising. As the chart below illustrates, obligations associated with the data attach to that data. New uses for data create new obligations for transparency and choice. Companies that provide data to other companies must have contracts in place that articulate obligations. They must also conduct appropriate due diligence to ensure that the company receiving the data possesses both the capacity and willingness to fulfill the obligations articulated in those contracts.

In the case of the hotel, each entity — the chain, the hotel, the independent service providers — would manage its data consistent with the Use-and-Obligations analysis of fair information practices. The decisions of each entity about the obligations must attach to the data, and be met by anyone using it. In a Use-and-Obligations model, each entity would enter into contracts that would specify the obligations related to data that flows between business partners.

Table C
Data Flow Rules Between Companies with a Use and Obligations Centered Approach



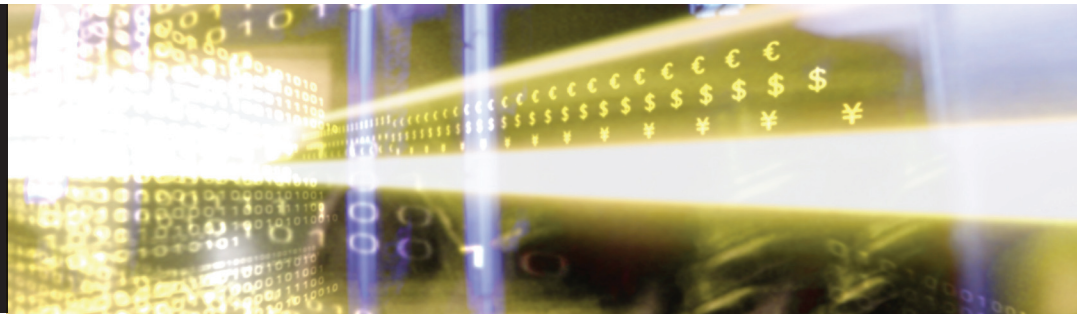
Contracts: The rights and obligations of parties sending and receiving data should be governed by contract. Companies that send data should conduct appropriate due diligence to ensure that organizations receiving data are willing and capable of meeting the obligations in law, regulation and company policy that come with the data. If data is transferred between companies to further a business process outsourcing arrangement, the outsourcing company must pass on the obligations via contractual requirements. If the data is transferred or sold downstream for multiple uses, the transferring organization must clearly articulate the nature of the obligations that attach to the data regarding each use.

Conclusion

A Use-and-Obligations model for implementing fair information serves an environment where data collection is ubiquitous and broad individual choice provides an increasingly less effective mechanism to trigger data protection obligations. By establishing data use as the basis for a data holder's obligations to protect data, a Use-and-Obligations model requires that organizations assess the risks to individuals raised by data collection and use, and take steps to mitigate those risks. Such an approach better informs consumers and provides their data with enhanced and more effective protection. It also sets clear expectations for organizations collecting and using data. Additional work must be undertaken to develop a practical framework for accountability. The Business Forum for Consumer Privacy encourages the necessary dialog and engagement to make an accountability approach to data protection a reality.

APPENDIX C

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



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

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

Data Protection Accountability: The Essential Elements
A Document for Discussion

Preface

Martin Abrams
Executive Director
Centre for Information Policy Leadership

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

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

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

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

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

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

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

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

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

Executive Summary

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

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

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

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

Accountability in Current Guidance

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

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

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

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

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

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

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

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

---

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

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

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

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

What is an Accountability-based Approach?

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

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

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

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

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

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

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

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

How Accountability Differs from Current Approaches

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

---

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

a) with the consent of the data subject; or

b) by the authority of law."

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

"An individual should have the right:

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

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

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

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

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

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

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

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

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

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

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

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

Essential Elements of Accountability

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

The essential elements are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Transparency and mechanisms for individual participation.

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

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

---

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

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

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

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

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

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

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

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

Public Policy Issues

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

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

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

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

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

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

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

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

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

---

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

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

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

3. How do regulators and accountability agents measure accountability?

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

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

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

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

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

(4) Transparency and mechanisms for individual participation; and

(5) Means for remediation and external enforcement.

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

Appendix
Galway Project Participants

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

Joseph Alhadeff, Oracle Corporation

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Marcus Belke, 2B Advice

Bojana Bellamy, Accenture

Daniel Burton, Salesforce.com

Emma Butler, Information Commissioner's Office, United Kingdom

Fred Cate, Indiana University, Maurer School of Law

Maureen Cooney, TRUSTe

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Peter Hustinx, European Data Protection Supervisor

Takayuki Kato, Consumer Affairs Agency, Japan

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

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Data Protection Commissioner, Spain

Rocco Panetta, Panetta & Associates

Daniel Pradelles, Hewlett Packard Company

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Scott Taylor, Hewlett Packard Company

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

K. Krasnow Waterman, Massachusetts Institute of Technology

Armgard von Reden, IBM Corporation

Jonathan Weeks, Intel Corporation

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

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

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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