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

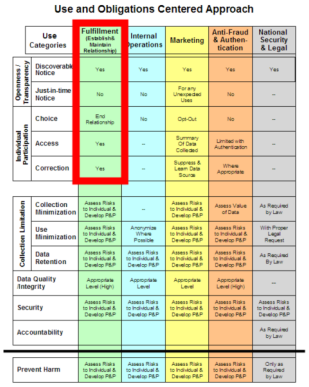
Table A offers a visual analysis of the Use-and-Obligations model. This section walks the reader through an analysis of each category of data use and the obligations triggered by that use. Part I of the analysis first examines the obligations related to individual participation. Part II reviews the internal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

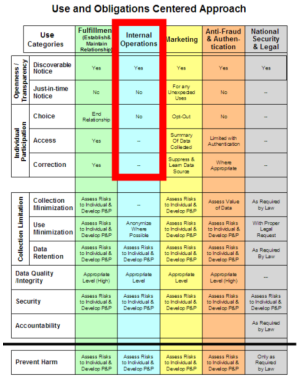


Transparency/Notice. Consumers must be provided a discoverable notice about data collection and uses for transaction fulfillment and service delivery. Just-in-time notice is not required, although consumers may appreciate such a notice for certain complex transactions or services.

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]

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

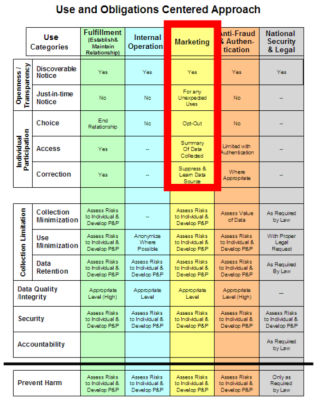


Transparency/Notice. Consumers must be given notice of data use for internal business processes. Just-in-time notice is not required, because consumers would not find the uses unexpected.

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.

Marketing



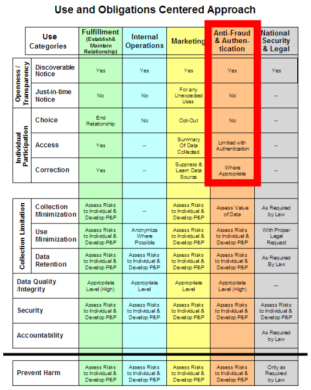
Transparency/Notice. Just-in-time notice must be provided if the marketing initiatives would not be expected by the consumer. For other marketing, companies must provide an easy-to-read, discoverable privacy policy.

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.

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



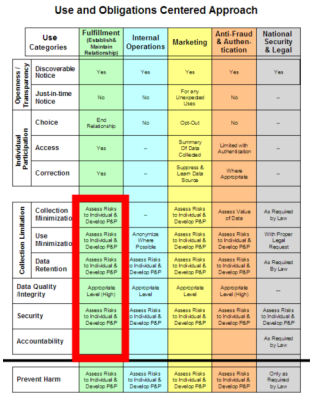
Transparency/Notice. Just-in-time notice is not required. However, the privacy policy must state that the data is used to prevent fraud.

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.

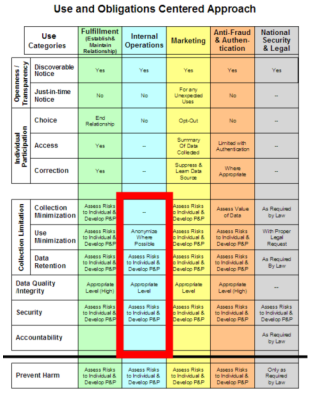
Data Quality and Integrity. Data related to fulfillment usually includes, among other things, name, address, and credit card data. Because it is important both to the organization and the individual that fulfillment data be correct, data quality requires that the organization ensure that the data be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

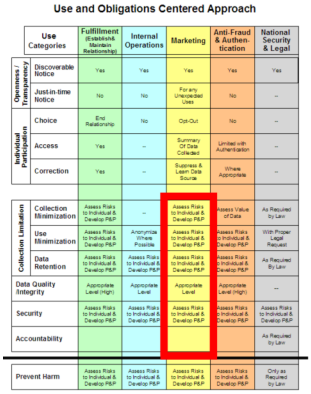
Data Retention. Organizations must determine how long data is needed, and assess the risks to individuals raised by retaining data. In light of that assessment, organizations should develop a schedules, policies, and procedures for retiring the data.

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 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.

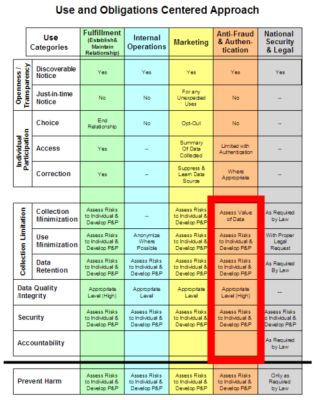
Accountability. Organizations must have in place policies, procedures, training, and compliance assessment to ensure that use of data for marketing is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

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.

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

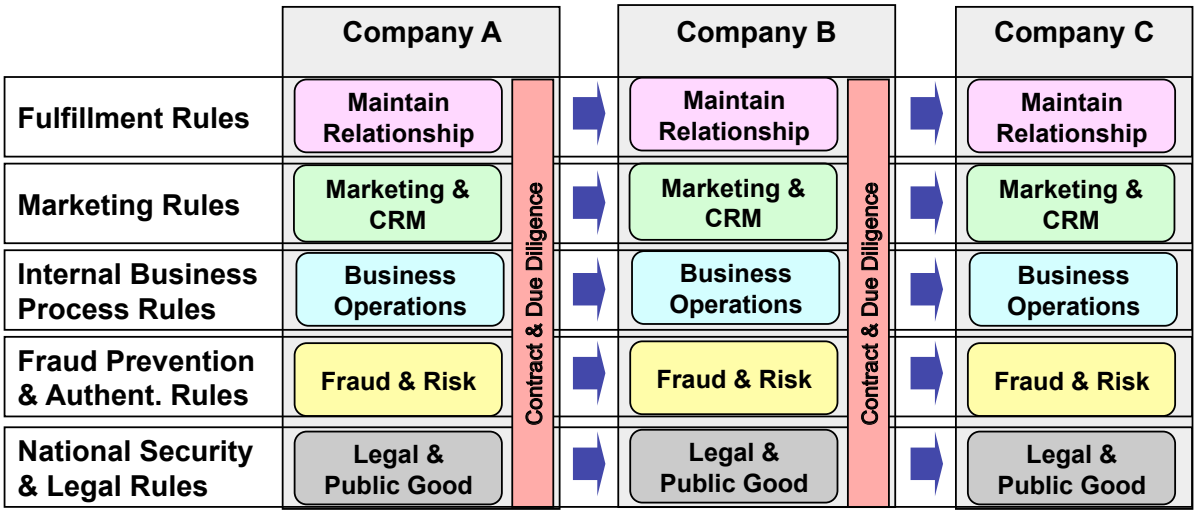
		Use Categories	Fulfillment (Establish& Maintain Relationship)	Internal Business Processes	Marketing	Fraud Prevention & Authen-tication	National Security & Legal
Part I -- Individual Participation	Openness / Transparency	Discoverable Notice	Yes	Yes	Yes	Yes	Yes
		Just-in-time Notice	No	No	No	No	N/A
	Individual 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.