RETHINKING PRIVACY:
FAIR INFORMATION PRACTICE PRINCIPLES REINTERPRETED

On the occasion of the 37th Annual International Data Protection and Privacy Commissioners' Conference, we are pleased to release "Rethinking Privacy: Fair Information Practices Reinterpreted."

This document, a product of Intel's Rethink Privacy initiative, encourages policymakers and industry leaders to continue to rely on the full complement of fair information practice principles to protect the privacy of individuals. At the same time, it recognizes the practical challenges practitioners face in applying these principles to emerging technologies and new data uses. We review each principle in turn, and consider approaches to their application that can work in this complex, fast paced technology and data environment.

The work of Rethink Privacy rests on the belief that assuring privacy and the protection of personal data is essential to the ability to realize the promise of big data and technology innovation. Privacy and innovation, therefore, are not values to balance or trade, but instead to pursue in tandem. We are privileged to release this document as government policymakers, data protection authorities, industry representatives, and advocates gather this week around the theme of the conference, "Privacy Bridges." We encourage participants to consider the ways in which fair information practice principles – reinterpreted to address the realities of 21st century technology and data use – can help us promote privacy and innovation by bridging protections across and between regions, cultures, technologies, platforms and individuals.

Technology and data-driven innovation hold the potential to advance education, medicine, good government, scientific research, disaster relief and smart cities in transformational ways. They hold the keys to solving longstanding societal problems. Intel looks forward to continuing to work with stakeholders to Rethink Privacy and to develop creative, effective approaches to data protection that make this promise a reality.

David Hoffman
Associate General Counsel
and Global Privacy Officer

Paula J. Bruening
Senior Counsel
for Global Privacy Policy

RETHINKING PRIVACY:
FAIR INFORMATION PRACTICES REINTERPRETED

INTRODUCTION

Principles of fair information practices ("FIPPs") have formed the foundation of data privacy guidance for over 40 years. By focusing on the collection, use and protection of information rather than on any particular technology, practice or application, the FIPPs have demonstrated their flexibility and adaptability. As a result, they have remained relevant over decades of transformational developments in the digital marketplace – in technology, business models, data uses and citizens' expectations. First articulated in 1973, FIPPs continue to serve as the basis for law and regulation across the United States, in Europe and around the globe. They also form the foundation for industry codes of conduct and international agreements about accepted data protection and transfer practices.[1]Intel relies on the articulation of the FIPPS in privacy guidelines developed by the Organization for Economic Cooperation and Development as the core of its privacy policies and practices. They were designed to harmonize national privacy legislation without interrupting the free flow of information across borders, and comprise eight principles that address the collection, security and primary and secondary uses of data.[2]

---

[1] Among the most widely recognized international agreements governing international data transfers is the Organization for Economic Cooperation and Development's "Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data," articulated in 1980. These guidelines were updated in 2013. The Asia Pacific Economic Cooperation forum adopted the APEC Privacy Framework in 2005. The Framework also relies on FIPPs as its foundation, but places emphasis on prevention of harm to individuals that might result from the misuse of information as one of its primary objectives. Commentary to the Framework states that protections and remedies for infringements should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information. Other iterations of the FIPPS have also gained relevance. For a review of the history of the FIPPs (albeit with a heightened though not exclusive focus on the United States), see Robert Gellman, "Fair Information Practices: A Basic History," version 2.12, August 3, 2014, at http:/www.bobgelman.com/rg-docs/rg-FIPShistory.pdf, last accessed January 19, 2015.

[2] The eight principles set out by the OECD are: 1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards principle; 6) openness principle; 7) individual participation; and 8) accountability, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," available at

Recently, traditional notions of FIPPs have come under scrutiny. Fast-paced developments in digital technology present unprecedented practical challenges for companies applying privacy law, regulation, and commonly accepted principles. Moreover, as analytics enhance and amplify the power of data processing and the insights it yields, organizations are required to make difficult choices about when data processing is appropriate and how to apply traditional guidance.

In spite of these concerns, Intel believes that the FIPPS continue to reflect long-held, widely-accepted values about the individual's relationship with personal data and organizations' responsibility to protect that data.

In early 2014, Intel released "Applying Privacy Principles in a Rapidly Changing World."[3]In that paper we assert that policymakers should not discard these enduring principles, but instead consider new methods of implementation that effectively protect privacy and encourage innovation. We suggest that traditional principles of fair information practices continue to provide relevant data protection guidance, but that they must be reinterpreted to keep pace with rapid innovation in technology and data use.

This paper further develops the discussion begun in the 2014 document. It expands on the ideas developed in that paper, and reflects on developments in privacy policy discussions that have taken place since then, most notably the White House release of the Consumer Bill of Rights Act of 2015.The essential theme remains the same, however: Fair information practice principles can continue to guide the ethical and innovative use of data when applied in a way that is practical and reflects the realities of the emerging data ecosystem. What follows proposes how that can be accomplished.

PRINCIPLES OF FAIR INFORMATION PRACTICES

1. **Collection Limitation Principle**

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

The Collection Limitation Principle traditionally has been interpreted to require that data controllers limit their collection to data that is necessary to complete a transaction or carry out a particular, identified function. According to this principle, the amount of information collected and held should be the minimum necessary to achieve the specified purpose.

The promise of big data and analytic processing challenges the traditional implementation of this principle, and has prompted some to question its continued relevance. The ability to derive powerful

www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface, last accessed December 27, 2014.

[3] "Protecting Consumer Privacy in an Era of Rapid Change," available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf, last accessed December 27, 2014.

predictions and insights from big data depends upon data scientists' access to vast, diverse sets gathered from a variety of sources. Data scientists sift and analyze this data to determine what it may reveal. They may or may not begin with a particular question they seek to answer, and often the correlations they glean are unexpected, or previously unknowable. More data, it is believed, provides more resources that can be mined for insights to provide benefits across all sectors of society – education, medicine, research, delivery of government services to citizens, business, international development, urban planning and energy conservation.

Some commenters suggest that strict application of the principle of collection limitation could reduce the amount of data available for analytic processing, and as a result, unnecessarily constrain the scope of data research and the benefits that may flow from it. They assert that the demands of big data require that the principle of collection limitation be substantially curtailed or eliminated. They argue that limiting data collection could preclude the discovery of important correlations that may not be anticipated today, but may be important in the future and revealed through advanced analytic processing.

In contrast, the White House draft legislation reflects a more traditional approach. It provides that an entity "may only collect . . . personal data in a manner that is reasonable in light of context." Such an approach allows some latitude for broader data collection, but may not support sufficient flexibility to advance the potential of big data analytics. Such limitations may unduly constrain companies' ability to lawfully collect data, and in doing so narrow the universe of data available for processing and therefore limit the potential benefits of big data analytics. Moreover, the provisions in the draft legislation that require the deletion, destruction or de-identification of data do not take into account the reality that data's usefulness may not be immediately apparent and may only emerge with the development of new algorithms or through analysis by data scientists.

Intel proposes a middle path that subjects decisions about data collection to risk analysis. Intel recognizes that collection of information can create risks for individuals. Security breaches provide an example of this type of risk, as unauthorized access to data can result in use of the information to harm individuals. In some cases the best way to minimize the risk may be not to collect the data in the first place. While the value of large, diverse data sets is well-recognized, societal norms or interests may argue against collection of certain kinds of information, if the risks outweigh the potential benefits.[4]

Rather than unduly limit data collection – or promote its unfettered collection - governance should support organizations assessment of the risk and benefits that may flow from the collection of data. Organizations should limit the collection of data that creates a high risk of harm either to individuals or to society, and where the potential benefits do not justify those risks. Intel expects that such high risk situations should be the exception instead of the rule. The default, therefore, should be that data can be collected, so that the potential to address pressing societal issues can be explored and realized.

[4] An example of such a risk might be a camera feed designed to capture images of individuals as they enter a medical clinic that primarily makes treatment available to people who are HIV positive.

When risk is assessed and an organization decides to collect data, appropriate strategies to mitigate attendant risks should be developed and followed. While the White House draft legislation suggests such risk mitigation strategies when it provides that a covered entity shall (among other things) 'de-identify' personal data. . . within a reasonable time after it has fulfilled the purpose or purposes for which such personal data were first collected," it is again important to recognize that the full breadth of data's value may not be immediately apparent, and its usefulness for analytic processing may reveal itself many years into the future. It will be important to tailor mitigation strategies to take this reality into account. Sweeping requirements that data be deleted, destroyed and de-identified could permanently eliminate important data sets that could yield important benefits.

Companies that look to risk assessment and mitigation to support decisions about data collection need a clear, reliable articulation of risk. Intel supports the work of experts, advocates, business and policymakers to understand the nature of risk in the digital environment, and to develop guidance about how it can be assessed.

2. **Data Quality Principle**

"Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

The Data Quality Principle promotes the use of data of a quality commensurate with the purpose for which it being used.

The Data Integrity Principle is reflected in the EU Data Protection Directive, which requires Member States to provide that personal data is, among other things, "accurate and, when necessary, kept up to date." It further requires that 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."[5]Similarly, the U.S. Privacy Act requires that government agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination[.]''[6] The principle is also found in international guidance on privacy and data protection and industry best practices.

The quality, relevance, and suitability of data fostered by the Data Integrity Principle continue to be important, particularly when data about individuals is processed using analytics. While the quality of data may be less critical when data scientists search for general trends in data, it remains essential when

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Section I, Article 6(d) provides that data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. . . "

[6] 5 U.S.C Sec. 522 a(e)(5).

data is processed to arrive at predictions or decisions that will affect an individual.[7]While data quality has always been important to arriving at trustworthy decisions, the enhanced power of analytics, the predictive insights it can yield, and its role in decisions about individuals in such fundamental areas as medical treatment, access to insurance, and academic and educational pursuits has heightened the importance of this principle. Companies using personal data to arrive at a decision affecting individuals should make sure that the data is relevant, accurate, complete, and up-to-date.[8]

Intel believes that it is important that governance focus on the *goal* of the data quality principle – the relevance and suitability of data for its intended use. Doing so will promote trust that data will result in appropriate, fair decisions and outcomes. While the White House draft legislation provides that organizations should "establish, implement and maintain procedures to ensure that personal data under its control is accurate" we believe that the focus should be on the suitability of data for its intended use and that a more nuanced approach is appropriate. We propose not that companies be required to keep *all* data accurate at all times, but rather to make sure that the data used is accurate to the extent necessary for its intended use.

Moreover, data analytics also highlights the importance that data be relevant for its intended use. While more data will be relevant to analytic processing that yields trends or correlations, not *all* data will be relevant for such uses. Analyzing whether data is relevant for the intended use remains critical to promoting data quality.[9]

The Privacy Act[10] takes this approach. It provides that any agency maintaining a system of records **"**maintain all records *which are used by the agency in making any determination about any individual* (emphasis added) with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." We believe that companies should

---

[7] K Krasnow Waterman and Paula J. Bruening "Big Data analytics: risks and responsibilities," *International Data Privacy Law*, 2014, Vol. 4, No. 2, Oxford University Press,
available at http://idpl.oxfordjournals.org/content/4/2/89.full.pdf+html, last accessed on December 27, 2014. Maintaining data at a level of a quality appropriate to its intended use is important to accountability, which makes companies responsible for understanding the risks involved with data use and for making decisions that promote good privacy outcomes.

[8] The access to data that promotes openness and individual participation also facilitates data integrity. Access and rights to correction or amendment provide individuals with the opportunity to review data pertaining to them and ensure its accuracy. This is discussed in more detail later in this paper.

[9] Such analysis is also key to the privacy review necessary for accountability. Understanding the extent to which data is relevant to for a particular use, and the potential impact of that use on individuals, is essential to the risk assessment and mitigation central to accountability, discussed later in this paper.

[10] The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

be required to use such a process to maintain the accuracy and integrity of data so that it is suitable for its intended use, with an understanding that over time more data will be suitable for intended uses.

3. Purpose Specification Principle

"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

The Purpose Specification Principle has been interpreted to require companies to limit their use of data to that specified in their privacy policy as made known to the user. It has allowed for uses compatible with that set forth in the privacy notice.

The challenges involved in understanding what uses an organization can make of data in the context of its privacy policy increase with the proliferation of new technologies and advances in processing capabilities. Big data analytics is an important example of how these developments heighten the focus on the purpose specification principle. Understanding what uses an organization can make of data in the context of their privacy policy is especially challenging when it is not possible to anticipate what insights analytic processing of data may reveal, and when the questions data may answer are only apparent years after its collection.

The Consumer Privacy Bill of Rights places purpose specification in the context of the company-consumer relationship. It refers to the need for companies to limit the use, collection and disclosure of personal data to those purposes that are consistent with both 1) the relationship that they have with individuals; and 2) the context in which individuals originally disclose the data, unless required by law to do otherwise. In its discussion of a company's analysis of context, it refers to the age and sophistication of the user, the need to distinguish personal data uses on the basis of how closely they relate to the purpose for which individuals use a service or application, and the business processes necessary to provide the service or application. It further highlights that the "adaptive uses of personal data" may be the source of innovation.

The Article 29 Working Party's opinion on Purpose Specification notes that the 95/46 Directive allows the processing of data for purposes that are "specified, explicit and legitimate," and "not incompatible" with the original purpose.[11]It articulates key factors to be considered when assessing whether a purpose is "not incompatible," including:

[11] The opinion also clarifies aspects of the requirement such as "further processing" of data, the notion of incompatibility, the methods of compatibility assessments that the data controller may employ; and the situations in which such an assessment is necessary.

- The relationship between the purposes for which the data have been collected and the purposes of further processing;
- The context in which the data have been collected and their reasonable expectations of the data subjects as to their further use;
- The nature of the data and the impact of the further processing on data subjects;
- The safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[12]

We need additional guidance about what constitutes compatible use. Innovative uses of data that will drive substantial social benefits should largely be "not incompatible" with most purposes specified to individuals. For example, medical research that may find a cure for an illness will most likely be "not incompatible" with the original collection of medical information. However, use of that same data to increase medical insurance premiums would likely fail this test. The factors articulated by the Article 29 Working Party may be helpful in this analysis. Consideration of these factors should be supplemented with an evaluation of the social value of the processing.

4. Use Limitation Principle

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [purpose specification principle] except:

a) with the consent of the data subject;
b) by the authority of law."

Data governance mechanisms have traditionally relied upon choice or consent to determine the appropriate use of data. Two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Sometimes individuals are empowered to tailor the nature of the information they reveal and the uses to which it will be put.

Discussions about choice and consent reflect a movement away from the user's ability and responsibility to exercise control over the collection and processing of data pertaining to them. The ubiquity of data collection and use make choice unwieldy if not impossible to implement in many situations; because data is so central to the ability to participate in public life choice is often illusory. Organizational accountability (discussed in part 8 of this document) shifts the burden of policing the data marketplace from the individual (and her ability to exercise choice) to the company.

[12] The opinion also discusses the concept of "predictability as relevant when assessing the compatibility of further processing activities. It states that "[i]n general, further processing cannot be considered predictable if it is not sufficiently related to the original purpose and does not meet the reasonable expectations of the data subjects at the time of collection, based on the context of the collections."

Data governance would benefit from a model based on three categories of uses: permissible, contextual and prohibited uses. Practical implementation of the principle of use limitation should rely on a clear examination and articulation of acceptable and prohibited uses. Permissible uses could range from commonly understood business uses of data to fulfill contract requirements, deliver a good or service, or facilitate routine internal accounting functions. Prohibited uses could include the discrimination of individuals based on the processing of data that may reveal or imply characteristics such as race, gender, age, or others that fall outside legal or societal norms. Another category of prohibited uses could be uses of data to discourage individuals from exercising their legally protected rights. An example of this category of prohibited use would be the use of data to target individuals who are likely to engage in political protest or dissent.

Determinations about data uses that fall between those clearly defined as permissible and prohibited should be based on a company's analysis of the benefits and risks to the user. Additional work must be carried out to identify risks against which new uses are analyzed. The use of review boards may be useful to companies to establish a mechanism to evaluate the risk assessment. These boards could include internal and/or external experts to help make these determinations. Depending upon the size of the company, and the scope of its data processing, it may make sense to use an outside group of experts. Many companies are already using such review boards, and a cottage industry of external experts who advise various companies has already developed. Formalizing requirements for review boards would further encourage development of this expertise and likely drive down cost for smaller companies to make use of such boards. However, any prescriptive requirements about the board should be avoided to allow companies maximum flexibility to create a board that best fits its need

The White House draft approaches the principle of use limitation in terms of what it refers to as "respect for context," providing that organizations can process personal data "in a manner that is reasonable in light of context." It enumerates 11 considerations that define the contours of "context." We strongly agree that companies should have latitude to use data in ways that, as referred to by European policymakers, further their legitimate business interests and are not incompatible with any uses specified in their privacy policies.

We are also concerned that organizations might be required to fulfill *all* of the characteristics described in the White House draft's definition of context. In some cases, not all of these would apply to all companies. We encourage flexible analysis which reflects the practical realities of an organization and its data processing and results in strong privacy protections.

5. Security Safeguards Principle

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."

The Security Safeguards Principle requires that companies deploy procedural and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Procedural measures include internal steps organizations take to limit access to data and ensure that those

individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

Security is a process: no one static standard can assure adequate security, as threats, technology and the measures available to protect against intrusions and compromises to systems constantly evolve. Security programs to protect personal data may vary depending on the nature of the data collected. Companies have been required to maintain a security program that is "appropriate to the circumstances."

Complex data environments and vast data stores heighten the importance of security. Technology's increased capacity to collect, correlate, and store data about individuals raises the risk of its exposure and misuse. The importance of protecting data to maintain its integrity is heightened, as data can reveal more sensitive insights that in some cases have significant, long-term consequences for individuals. Moreover, the function and accuracy of critical systems operations will increasingly rely on data, further increasing the importance of security.[13]

Intel believes that organizations must implement appropriate administrative, technical and physical security measures that ensure the integrity and confidentiality of information and protect against threats. Security should also protect against unauthorized access to and loss, misuse, alteration or destruction of data. While the White House draft legislation proposes factors that should be considered in determining whether a company has implemented reasonable security[14]and the basic internal practices a company should implement,[15]Intel believes that the industry would benefit from security best practices developed through an industry-led process. Such best practices should take into account the size and complexity of an organization, the nature of its activities, risks in the use or transmission of data and the sensitivity of data in question. Best practices should also take into account the state-of-the-art safeguards available, cost of implementation, and best practices developed through multi-stakeholder processes.

6. Openness Principle

[13] Increasingly data will be critical to *inter alia* the accurate operation of personal medical devices; the safe operation of vehicles and movement of traffic on highways; and the appropriate, timely distribution of energy resources. See generally, Mayer-Schonberger, V. and Cukier, K., *Big Data: A Revolution that Will Change the Way We Live, Work and Think,* Clays Ltd., St. Ives plc, 2013.

[14] The White House draft legislation sets out the following factors: the degree of the privacy risk associated with the personal data; the foreseeability of threats to the security of the data; widely accepted security practices; and the cost of implementing and regularly reviewing such safeguards.

[15] The White House draft legislation also proposes that companies: identify foreseeable privacy and security risks to data; establish security safeguards; regularly assess the sufficiency of safeguards implemented; and evaluate and adjust safeguards in light of that assessment.

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller."

The principle of openness was originally articulated in the Code of Fair Information Practices developed by the Health Education and Welfare Advisory Committee. Their code stated that "[t]here must be no personal data record-keeping systems whose very existence is secret."[16] Beginning in the late 1970's, notice served to give practical effect to the principle of openness. Since then, notice has provided the basis for individuals' decisions about the collection, processing, sharing and reuse of their personal information. In the United States, it has served as the basis for regulation by the Federal Trade Commission under Section 5 of the FTC Act,[17] which provides that companies whose practices are at odds with their notices may be prosecuted for deception. The European Data Protection Directive specifies information about data collection, processing and sharing that must be provided to individuals.[18]The APEC Privacy Framework states that data controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information.[19]

---

[16] The Health, Education and Welfare Code of Fair Information Practices is based on five principles: 1) There must be no personal data record-keeping systems whose very existence is secret; 2) There must be a way for a person to find out what information about the person is in a record and how it is used; 3) There must be a way for a person to prevent information about the persona that was obtained for one purpose from being used or made available for other purposes without the person's consent; 4) There must be a way for a person to correct or amend a record of identifiable information about the person; and 5) Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

[17] Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits ''unfair or deceptive acts or practices in or affecting commerce.''

[18] Directive 95/46/EC Section IV, Article 10 states that, "in cases of collection of data from the data subject Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

[19] The APEC Privacy Framework notice principle provides that, [p]ersonal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

Notice arguably fosters openness by requiring companies to make public the business models, vendor relationships and the data practices that drive the digital economy. However, since the mid-1990's, both online and offline notices have come under criticism from regulators, privacy and consumer advocates, and businesses as too complex, legalistic, lengthy, and opaque. Businesses complain that drafting notices that meet regulators' requirements for completeness is difficult. Consumer advocates call for more clarity and concise, consumer-friendly language. Notices which support consumer choice about subsequent use of personal information often are written in language that allows companies such latitude that consent authorizes nearly any data use. Many notices are designed such that when an individual proceeds with the use of the service or website, consent is implied. Research shows that the great majority of individuals do not read privacy policies. Further it is unclear whether even those who do read them understand what they need to know about how their data will be processed.

Rapid changes in technology further strain the ability of companies to provide useful notice. Ubiquitous deployment of sensors, advances in big data and real time analytics, and the complex vendor relationships and data sharing partnerships that characterize today's information ecosystem challenge businesses' ability to explain their data practices. The need to use data robustly and in innovative ways clashes with requirements that notices specify a particular purpose or use for data collected. The extent to which data collection is integrated into infrastructures (such as intelligent vehicle highway systems) or environments (such as workplaces or medical centers) can make posting notice difficult, and new technologies such as mobile devices with small screens create new challenges for providing meaningful notice. As the amount of data that is supplied by someone other than the data subject (e.g., through social media) continues to grow, the effectiveness of traditional notice is further tested.

Given these challenges, some argue that notice requirements should be significantly limited or eliminated entirely. Intel disagrees. We believe that transparency serves a diverse set of purposes.

> **It serves as a basis for regulatory oversight**. In the United States, Section 5 of the Federal Trade Commission Act empowers the FTC to investigate and halt any "unfair" or "deceptive" conduct in industries affecting interstate commerce. This authority includes the right to investigate a company's compliance with its own asserted data protection policies. The FTC acts under this power to investigate organizations whose practices do not conform to the policy articulated in the privacy notice and to provide oversight and enforcement for the U.S. self-regulatory regime in the absence of omnibus privacy law.
>
> **It supports consumer privacy decisions.** If choice or consent is available, the information in a notice about a company's data practices helps individuals decide whether to engage with the organization or to allow subsequent uses of the personal information. Ideally, notices also enable individuals who value privacy to compare the practices of different organizations.
>
> **It supports the public dialog and oversight related to privacy**. Notice provides a tool for advocates, experts and the press to exercise their own oversight.

We believe that in the data environment we are creating, openness requires enhancing and building upon traditional notices to achieve *transparency.* Transparency encourages companies to investigate, understand and disclose what data they collect and hold, how and why they use it, whether and for how long they maintain it, and how they secure and protect it. Transparency involves complete and thorough explanation of data processing and protection practices *and* selective and targeted notice. Taken together, these can accomplish transparency by giving individuals, advocates and experts access to information about an organization's data collection practices, use of technology, and privacy protection measures. They can also continue to provide regulators with a basis for enforcement.

Transparency and notice may best be realized through their implementation of two kinds of communications:

> **Comprehensive disclosures**, which provide an in-depth explanation of how an organization collects, processes and protects data. Civil society, advocates, and experts may review these notices to develop a detailed view of a company's practices or gain an understanding of developments across the digital marketplace. Regulators may compare these statements with the company's activities to determine whether their representations are valid and whether their practices fall within the bounds of law and commonly accepted guidance.
>
> **Context-specific notices,** which provide concise, targeted information about data collection, use, storage and protection so individuals can determine whether to make a purchase, engage in an activity or interact with an online vendor. Focused, tailored, context-specific notices that are made available to the consumer at the appropriate time support individuals' real-time decision making about collection and use of their data.[20]

To best serve the public, notices should be supplemented with consumer education – a shared responsibility of industry, government and civil society – to provide additional opportunities for the public to understand their choices, when they should demand them, and the consequences of their decisions.

7. Individual Participation Principle

"An individual should have the right:

a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive in a reasonable manner; and in a form that is readily intelligible to him;

[20]For example, smart phone apps may provide an opportunity for consumers to exercise choice about whether to provide location data to a smart phone application, and at that time the information necessary to make that choice.

c) *to be given reasons if a request made under (a) or (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."*

Organizations traditionally have relied on access and correction-deletion to implement individual participation. Access as defined in the FIPPs includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. To be useful to the consumer, access must be inexpensive and timely.

Access is essential to improving data accuracy, which benefits both data collectors who rely on such data, and individuals who might otherwise be harmed by adverse decisions based on incorrect data. It also makes data collectors accountable to individuals for the information they collect and maintain about individuals, and enable individuals to confirm that websites are following their stated practices.

To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate, irrelevant, excessive or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections-deletions and/or consumer objections can be added to the data file and sent to all data recipients.

Access traditionally has proven to be a challenging issue. Companies have often resisted access requirements, citing the burden that responding to requests would entail, particularly as data stores have grown in size. They have also cautioned that providing access would involve authenticating the identity of individuals seeking access to data, and in doing so in some cases pose new privacy challenges. Organizations have also raised concerns about the extent to which providing access might reveal proprietary information.

Access-Correction/Deletion continues to be important to individual participation. When processing data affects decisions about an individual, the ability to correct, delete or amend information is needed to promote accurate, relevant, proportionate and current results. But in an environment where data stores are vast and the uses of data are varied, access rights should be reasonable and correspond to risk.

The White House draft provides for broad access rights, but also appropriately limits the degree and means of access based on the extent and nature of the risk that data raises and the cost of providing access. It further takes into account issues related to the ability to verify the identity of the person requesting access, limitations to access based in law or the requirements of law enforcement, and frivolous requests.

Intel believes that in cases of sensitive data or data that can be used to make a decision that affects the individual in some significant way, access to specific information and the opportunity to correct, delete, challenge or amend the data is necessary. (Exceptions to the ability to correct, delete and amend exist, e.g., in the case of credit reporting or criminal records, when there is an overriding public policy interest.) In cases where the use of data will not result in a decision that significantly affects the

individual, access by way of notice (where a company informs the individual of what data is held about him) may be appropriate.

Considerations relevant to when data should be deleted or suppressed will continue to pose challenging issues. The Fair Credit Reporting Act provides that it is impermissible to use certain data past a set time period.[21]European law reflects the notion that some data about an individual may be so excessive in its extent or effect on the individual that the data subject should have the ability to ask search engines to delete or obscure it. Given the increased percentage of information that relates to individuals but that does not come directly from data subjects, it is important for stakeholders to develop principles that allow a limited right to request deletion of even truthful data. It is critical that the goals of these principles also include preserving, if not enhancing, free expression. Allowing a limited right to delete inadequate, irrelevant or excessive data may foster free expression by removing the chilling effect that may result when individuals must worry that everything they say, do and even think may be stored forever and accessed by anyone.

8. **Accountability Principle**

"A data controller should be accountable for complying with measures which give effect to the principles stated above."

Over the past 30 years, laws, codes of conduct and international agreements addressing data protection and privacy have incorporated the principle of accountability. While the principle is not new, there is growing interest on the part of companies, regulators and lawmakers in how it can be more effectively used to promote and define organizational responsibility for privacy protection.

Binding Corporate Rules (BCRs) are an accountability-based instrument that facilitates cross-border transfers of personal data and protects personal data processed outside of the EU. BCRs are codes that protect personal data in such transfers. A key element of BCRs is that the "guiding nature of the rules in practice . . . would imply that the members of the corporate group, as well as each employee within it,

[21] Except as authorized under subsection (b), no consumer reporting agency may make any consumer report containing any of the following items of information:

> (1) cases under title 11 of the United States Code or under the Bankruptcy Act that, from the date of entry of the order for relief or the date of adjudication, as the case may be, antedate the report by more than 10 years.
> (2) Suits and judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period.
> (3) Paid tax liens which, from date of payment, antedate the report by more than seven years.
> (4) Accounts placed for collection or charged to profit and loss which antedate the report by more than seven years.
> (5) Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years.
> (6) Any other adverse item of information which antedates the report by more than seven years.

will feel compelled to comply."[22]Companies are required to demonstrate such compliance to the appropriate data protection authorities.

Accountability is a key component of Cross-Border Privacy Rules (CBPRs), a mechanism to implement the principles of the APEC Privacy Framework. CBPRs include a role for accountability agents, which may include trust marks, seals and other private bodies.

Recently, companies and regulators have engaged in a long-term effort to define the contours of accountability. In an accountability model, companies charge a person or team with responsibility for the privacy program. Within that program, companies are required to establish policies that foster the protection of individual privacy and to put in place processes and practices that further the effective implementation of those policies. Accountability focuses on setting privacy-protection goals for companies based on established public policy and allowing them discretion to determine how those goals are met. It requires that in making decisions about data collection, processing and protection companies assess the risks data use poses for individuals and take appropriate steps to mitigate that risk. When asked to demonstrate the steps they have taken to be accountable, organizations will be evaluated on the effectiveness of their internal processes and the credibility of their risk assessment.[23]

Accountable businesses adopt methods and practices to reach those goals in a way that best serves their business models, the requirements of technology, and the demands of customers. In exchange, accountability requires organizations to be prepared to demonstrate responsible policies and systems that effectively protect individuals and their data.[24]

Accountability best practices can be a useful tool for legislators and regulators. Lawmakers may provide safe harbor protection or mitigation of sanctions for companies who can demonstrate that they meet the requirements of accountability in their privacy programs and practices.[25]Those same best practices can also serve as an important enforcement tool for regulators who may require companies who have

---

[22] "Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Article 29 Data Protection Working Party, 3 June 2003, 11639/02/EN WP 74

[23] "Demonstrating and Measuring Accountability: A Discussion Document," Centre for Information Policy Leadership as Secretariat for the Accountability Project, October 2010, available at http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF, last accessed December 29, 2014.

[24] Ibid.

[25] Article 45 of the Spanish law establishes the amount of sanctions depending on the nature of the infringement. Article 45.4 establishes the criteria that would qualify an organization for a statutory reduction in the amount of the penalties. Such considerations would include the nature of the personal rights involved, the profits gained, the degree of intentionality, damages, et al., Among the criteria recently included is the existence, prior to the infringement, of adequate procedures and protocols in the collection and processing of personal data. If the infringement is a consequence of an anomaly in the functioning of those procedures and not a consequence of a lack of diligence, it would qualify an organization for a reduction under the statue.

not lived up to their responsibilities related to personal data to employ accountability mechanisms.[26]It will also be important that any legislation appropriately take into account the needs of small and medium sized enterprises. To promote accountability across industry sectors and the data eco-system as a whole, all organizations will need to be accountable. SMEs should be provided with effective incentives to adopt policies, programs and practices that promote privacy. Legislation should also promote development of tools that will help SMEs practically and effectively meet the requirements of accountability in a way appropriate to their size, business model and processing activities and extent and sensitivity of their data holdings.

APPLICATION OF THE FIPPS IN A DYNAMIC DATA ENVIRONMENT: A SYSTEMIC APPROACH

While an analysis of each of the FIPPs is necessary to any reconsideration of how they might be applied in the emerging data ecosystem, it is important to remember that simple adherence to each individual FIPP does not necessarily result in sound privacy protection. It is possible, for example, to deploy notice and require consent, and still leave the individual with little, if any, confidence that their data will be used and safeguarded responsibly. And in a technological, data-rich environment that changes rapidly and in often dramatic and unexpected ways, the manner in which the FIPPs are applied in their entirety will determine how effectively they protect the individual. Moreover, by applying FIPPs in a holistic or systemic way, companies can enhance privacy protections while unleashing the full innovative power of data.

Some data uses do not lend themselves to strict application of the full complement of the FIPPs. For example, smart energy systems may collect data from households that may reveal the habits and patterns of daily activities of the people who live there. That data can yield important predictions and analysis of demand that can aid in resource distribution, making electrical power, for example, available to the right areas of a municipality in the right volume at the right time of day or night. The shared benefits that can flow from such a capability are significant, and individuals and households may not be able to choose whether or not to participate in such a program. In light of that, collectors and users of the data should provide heightened transparency, security safeguards and accountability. Because much of the data and the results of its analysis could be considered sensitive when not aggregated, companies should provide requisite security and engage in rigorous risk assessment and mitigation in determining whether to use the data in a particular way.

In this way, the FIPPs can be viewed as a system of levers to be pulled and adjusted, or requirements to be given the weight necessary to provide the best protection possible in the context of a particular technology or data application. The heightened focus on accountability places greater burden on companies to make thoughtful, judicious decisions about how best to apply FIPPs in a way that practically yields effective protections.

[26] See e.g., *In the Matter of Facebook,* Docket C-4365, July 27, 2012, in which the FTC requires Facebook to, *inter alia* establish and implement a comprehensive privacy program that includes a designated employee or employees responsible for the program; engage in risk assessment and mitigation; and take reasonable steps to select and retain service providers capable of appropriately protecting the privacy of information.

Critical to this new vision for FIPPs is greater clarity and guidance about risk of data use to the individual and to society. As noted throughout this paper, many of the decisions we make about how FIPPs can most effectively be applied will rely on understanding, assessing and mitigating the risks that data processing may raise for individuals. Companies will need a clear articulation and legal certainty about the risks against which they will measure these decisions. While some of these are well established – risk of financial or physical harm, for example – others may be less defined. It is imperative that the work of experts, advocates and policymakers continue to better understand the contours of risk in the evolving data environment and develop this guidance.

CONCLUSION

This paper represents a further step in Intel's effort to reinterpret the FIPPs in a way that serves the privacy interests of individuals and creates an environment that fosters innovation and the responsible, robust use of data. Because FIPPs require practical implementation, it will be necessary to answer critical questions, among them: Against what risks should companies evaluate their possible uses of data? Who within companies makes decisions about the use of data for analytic processing? Which data uses are allowed and which are prohibited? What criteria should companies use to determine when analytic processing is appropriate? Resolving these issues is hard work and demands collaborative thinking. Intel would like to continue this discussion by asking for comments on this paper on our policy website https://blogs.intel.com/policy/, where we will continue to Rethink Privacy.