THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

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

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

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

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

January 28, 2011

Office of the Secretary
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

Re: Docket No. 101214614-0614-01
"Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"

Dear Sirs and Madams:

The Centre for Information Policy Leadership ("the Centre") appreciates the opportunity to respond to questions posed in the Department of Commerce ("the Department") Internet Policy Task Force document, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." The Centre commends the Department on the release of its policy framework and on undertaking this important effort.

The Centre's mission is development of forward-thinking information policy for a digital economy. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, accountability-based governance, development of privacy law in emerging economies, and government use of private sector data. The Centre has worked extensively with business, advocates, experts, congressional staff and international organizations on issues of privacy and data protection.

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

1. The Policy Framework should rely less upon the individual's control over the collection and use of data about him and more upon data stewardship and organizational accountability.

The Policy Framework proposed by the Department relies heavily upon a model based on the individual's ability to control the collection and use of data pertaining to him or her. This approach was anticipated when principles of fair information practices were originally articulated in the 1970s. In that early iteration, the principles were designed to provide individuals with sufficient information about how data about them would be collected, used, shared and stored. On the basis of that notification, individuals could choose whether to share data or to do business with an organization.

While individual control has traditionally motivated application of fair information practices, such an approach is no longer sufficient to protect individuals. The rate at which data proliferates today is vastly greater than it was in the 1990s, when the Internet emerged as a commercial medium. Data is collected from consumers in places and ways not anticipated even five years ago. Use of data about individuals has become so central to his or her ability to engage in basic life activities that choice may not always be an option. As the complexity of data collection practices, business models, vendor relationships and technological applications grows, it often outstrips the individual's ability to make decisions to control the use and sharing of information through active choice. While individual control remains important in some instances, such as when the data or the data use is sensitive or raises particular risks to individuals, control can no longer serve as the primary motivator of consumer privacy protection in every circumstance.

Moreover, the current environment of fast-paced innovation in technology and data applications is not well served by a control model. To be competitive, and to respond to consumer demand, organizations need to be able to use data in new ways, while still being responsible. A model that requires consent for each kind of data use may severely restrict organizations' ability to make decisions about data use that allow them to respond quickly to the market.

The Centre recommends that the Department consider instead an approach to data protection that relies upon organizations' accountability for the responsible management and protection of data. Accountable organizations implement mechanisms to ensure responsible decision-making about how data is optimally managed and safeguarded based on credible risk assessment. Such an approach requires that organizations commit to being responsible and answerable for their data collection and management decisions. They must put in place policies based on established external criteria and deploy mechanisms that implement those policies and measure their effectiveness.

Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing an increasingly complex, rapidly changing marketplace for enterprises using data irresponsibly. Accountability requires responsible data use whether or not a consumer has consented to one use or another. It also allows for flexible data use based on a realistic assessment and mitigation of the risks involved that enhances opportunities for innovation.[1]

2. The Department should look to fair information practice principles as articulated in the OECD Guidelines as the foundation for privacy guidance.

The Centre agrees that in the current environment, application of a more comprehensive articulation of fair information practices is necessary to provide robust data protection. Adoption of a more complete set of fair information practice principles, while not an attempt to mirror other regimes, would create greater possibilities for interoperability with approaches in other regions. The Centre encourages the Department to adopt the OECD Guidelines[2] as the foundation for private sector guidance. Recognizing that guidance must keep pace with changes in technology, business processes and data applications, the Centre notes that the OECD Guidelines were developed in a technology-neutral way to encourage privacy, innovation and economic growth. There are numerous efforts under way to adapt the OECD Guidelines to respond to dramatic changes in information technologies and applications. The Department has helped lead one of the most successful as a part of its work on the Asia Pacific Economic Cooperative's Privacy Framework. The Centre is sponsoring another effort to fine-tune the OECD Guidelines to reflect the realities of 21st century data collection, processing and retention. (The attached discussion document by Professor Fred Cate, Senior Policy Advisor at the Centre, provides an introduction to that effort, and is intended to serve as a discussion platform within the Centre and with other stakeholders.) The OECD itself is now reviewing its Guidelines in a process in which the United States participates. We encourage the Department to look to these broader efforts.

3. Principles of fair information practices should be applied within a contextual framework, and not in a rigid or fixed way.

The Centre cautions against applying fair information practice principles inflexibly. Instead, they should be applied within a contextual framework in which different principles carry more

[1] An accountability approach is consistent with the framework on which the federal Fair Credit Reporting Act is structured and the manner in which bank regulators oversee data use governed by the Act. Both require that data collectors and users operate within a set of established legal requirements, and both place responsibility for appropriate data use and management on organizations rather than on individuals.

[2] The Organization for Economic Cooperation and Development issued its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

importance depending on the nature of the data, its sensitivity, or how it is used. For example, enhancing cyber security requires robust collection of information to predict risk and identify legitimate and rogue users of the networks. Application of the principle of collection limitation may be applied less rigorously in such instances. However, given the robust nature of the collection and the potential sensitivity of identifying information, an organization would be expected to implement security in a manner that addresses the risks raised by the collection, use and retention of that information.[3]

4. The Centre encourages organizations' use of privacy impact assessments as a tool to assess and manage risks that data use may pose to individuals. However, such assessments are not the appropriate tool to serve the transparency function suggested in the Department's framework.

Organizations have used privacy impact assessments to manage risks to individuals since as early as 1993. They are an essential tool for organizations as they put privacy protections into place and test new products, services and processes for risk to individuals. They are also key to an organization's decisions about implementing appropriate privacy protections. Many organizations conduct hundreds of privacy impact assessments every year.

In limited instances, privacy impact assessments can enhance transparency about an organization's data practices. For example, to address public concern about an emerging technology or business offering, it may be appropriate to make a privacy impact assessment available to the public for purposes of education or to enhance consumer trust. However, as a general rule privacy impact assessments carried out in the private sector are not intended to serve as a transparency device, and publication of the findings of a privacy impact assessment, as suggested in the Department's framework document, is not appropriate.[4] In the vast majority of cases, privacy impact assessments are part of a broader *internal* assessment process and form part of the basis for decisions within the organization. An organization may conduct a privacy impact assessment and determine that a proposed application or business model raises risks to individuals that the organization cannot tolerate or mitigate appropriately, and consequently decide not to move forward. Or it may carry out an assessment, and based on its findings modify its new offering to reduce its customers' exposure to risk.

[3] The application of analytics to large data sets in an effort to understand trends and predict future events represents another area where fair information practices should be applied in a manner that reflects the context of the data use. In his recent paper, "Data Protection Law and the Ethical Use of Analytics," Professor Paul Schwartz raises concerns about the appropriate application of principles of collection minimization and use limitation when an organization uses analytics to better understand what insights data might yield.

[4] The Centre recognizes that privacy impact assessments have been used as a transparency tool in the public sector and recognizes their value when used in this way. However, such documents are often highly nuanced and carefully reviewed and revised prior to their publication, and their use by government does not argue for their use by private industry where considerations related to the data may differ markedly.

Privacy impact assessments may contain significant amounts of proprietary information, and its publication could reveal to competitors information about new products, services and offerings. Organizations might therefore be persuaded to oversimplify or sanitize privacy impact assessments or to generate versions of reports that avoid any liability or compromise to reputation. Furthermore, requiring organizations to make the results of all of their privacy impact assessments public might discourage organizations from carrying them out at all and deny industry the benefits of privacy impact assessments.

The Centre believes that privacy impact assessments should continue to serve as an important tool for responsible organizations that wish to base their data management decisions on a clear understanding of privacy risks their products, services and technologies raise. The Centre is concerned that, should they be made public as required by the Framework, organizations will limit their use and lose the advantage of the important insights they provide.

5. While the Centre encourages the establishment of a Privacy Policy Office in the Department of Commerce, it cautions that its charter should be clear and appropriate. Development of voluntary codes of industry conduct is best carried out by the organizations affected in a non-government environment that encourages candid and open negotiation.

The Centre has long encouraged establishment of an non-regulatory, Executive Branch office focused on consumer privacy. We suggest such an office could appropriately identify issues, conduct research, encourage common approaches to commercial privacy protection among government agencies, convene forums and meetings to explore contentious issues, encourage development and facilitate vetting of safe harbor programs, and stay abreast of how business processes and technologies are emerging and evolving over time.

The Centre is concerned that, as described in the proposed framework, the office would become inappropriately central to development of codes of conduct. While it is appropriate for such an office to motivate industry to develop those codes and encourage engagement of all stakeholders in the development process, the codes must be voluntary, and stakeholders will need a forum for frank, candid deliberation and negotiation that does not involve observation or comment by government and/or media. It will of course, be necessary for such an office to set goals, define the contours of such guidance, receive progress reports and vet the product. But the process must be run, and the pen held, by the interested stakeholders who will need to abide by the codes of conduct.

6. We recommend that the privacy office take a lead role in discussions in international organizations, and that the Federal Trade Commission continue to represent the United States in forums concerned with privacy regulation.

The Department of Commerce has played a key role in privacy policy development through its work at the OECD and the Asia Pacific Economic Cooperation, and in bilateral negotiations and trade discussions. It has served as an effective, trusted representative for US interests in that capacity, and we encourage the Department to continue in that role.

We commend the partnership that has emerged between the Department and the Federal Trade Commission as they fulfill their respective roles in privacy deliberations in international forums. The Federal Trade Commission's position as the point organization in forums oriented to regulatory issues and that require the participation of a regulatory authority -- such as the International Conference of Data Protection and Privacy Commissioners, the Article 29 Working Party, and other international privacy regulatory organizations -- remains important to the success of U.S. efforts.

Conclusion

The Centre appreciates this opportunity to participate in the Department's work to address issues of commercial data privacy. We hope that the Department will look to the Centre as a resource, and are available to provide further information or to elaborate on the comments above. Please direct any questions to Martin Abrams at mabrams@hunton.com or Paula Bruening at pbruening@hunton.com.

Yours sincerely,

Martin E. Abrams
Executive Director

Paula J. Bruening
Deputy Executive Director

APPENDIX

UPDATING THE OECD GUIDELINES FOR THE 21ST CENTURY: FIRST THOUGHTS

Fred H. Cate[1]

The OECD 1980 Guidelines

Modern data protection law is built on "fair information practices." According to Professor Paul Schwartz, a leading scholar of data protection law in the United States and Europe, "[f]air information practices are the building blocks of modern information privacy law."[2] Marc Rotenberg, president of the Electronic Privacy Information Center, has written that "Fair Information Practices" have "played a significant role" not only in framing privacy laws in the United States, but in the development of privacy laws "around the world" and in the development of "important international guidelines for privacy protection."[3]

One of the earliest and broadest efforts to identify the principles necessary to strike the delicate balance between privacy and the responsible use of information was led by the Organization for Economic Cooperation and Development ("OECD"). The OECD Committee of Ministers' 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[4] ("Guidelines") identified eight principles to "harmonise national privacy legislation and, while upholding such human rights, ...at the same time prevent interruptions in international flows of data."[5] They were designed to "represent a consensus on basic principles which can be built into existing national legislation" and to "serve as a basis for legislation in those countries which do not yet have it."[6] In this aspiration they have undoubtedly succeeded because most of the dozens of national and regional privacy regimes adopted after 1980 claim to reflect the OECD Guidelines.

The Guidelines' eight principles are:

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.

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.

---

[1] Distinguished Professor, C. Ben Dutton Professor of Law, Director of the Center for Applied Cybersecurity Research, Director of the Center for Law, Ethics, and Applied Research in Health Information, Indiana University; Senior Policy Advisor, the Centre for Information Policy Leadership at Hunton & Williams LLP. The author alone is responsible for the views expressed herein.

[2] Paul M. Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1607, 1614 (1999). Professor Schwartz describes FIPPS as being "centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight." *Id.*

[3] Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get," 2001 *Stanford Technology Law Review* 1 ¶ 43.

[4] O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

[5] *Id.* at preface.

[6] *Id.*

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.

4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
   a. with the consent of the data subject; or
   b. by the authority of law.

5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle—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.

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

8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.[7]

Under the OECD Guidelines, data processors have certain obligations without regard for the wishes of individual data subjects. For example, the data quality and security safeguards principles appear non-negotiable. Other obligations focus significantly on individual consent. For example, under the use limitation and purpose specification principles, the use of personal data is restricted to the purposes for which the data were collected, purposes "not incompatible with those purposes," and other purposes to which the data subject consents or that are required by law. Still other principles—for example, the openness and individual participation principles—are designed entirely to facilitate individual knowledge and participation.

[7] *Id.* ¶¶ 7-15.

New Challenges to Protecting Privacy

A great deal has changed since the OECD adopted its Guidelines in 1980. Advances in digital technologies have greatly expanded the volume of personal data created as individuals engage in everyday activities. "With the rise of new networks," *BusinessWeek* wrote in its August 28, 2008, cover story, we are "channeling the details of our lives into vast databases. Every credit-card purchase, every cell-phone call, every click on the computer mouse [feeds] these digital troves. Those with the tools and skills to make sense of them [can] begin to decipher our movements, desires, diseases, and shopping habits—and predict our behavior."[8] The data routinely generated, collected, and stored include:

- What individuals buy and the other transactions in which they engage through 30 billion checks, 26 billion debit card transactions, 22 billion credit card transactions annually.

- What individuals communicate with family, friends, and colleagues in more than 30 billion emails a day. We send 173 billion text messages per month. These are all captured digitally, together with voicemail and Voice Over IP conversations, by someone other than, or in addition to, the sender.

- Location information. As of 2010, there are 5 billion mobile phones worldwide—almost double the figure just four years ago—which 95 percent of users say they keep within three feet of themselves at all times. Mobile phones thus constitute the world's largest sensor network. Through GPS and triangulation, these phones generate increasingly precise information about the location, speed, and direction of movement of the user. Many cars contain navigational systems that include a GPS receiver. Laptops, PDAs, and cell phones that connect to WiFi necessarily provide information concerning the user's location. Electronic toll payment systems provide a stream of location data to anyone with an appropriate reader.

- What individuals watch, listen to, and read through digital satellite and cable, iTunes, Amazon, and hundreds of other entertainment service providers and vendors.

- What individuals are doing in the office, in public, and increasingly even at home with video and audio surveillance, key-cards, security systems, keystroke monitoring, stored email and voicemail, and remote access to networked files. In 2006, 200 traffic surveillance cameras in London sent 8 terabytes of data a day to the central command center.

- What individuals are interested in, looking for, or concerned about. As of fall 2010, Internet users generated about 113 billion searches a month, doubling every two years, and visited an estimated 255 million websites, 15 times the number a decade earlier.

- Data on individuals and their families, friends, and co-workers through social networking, 152 million blogs, photo and video sharing, peer-to-peer file-sharing, virtual worlds, and even remote storage of documents and financial information—what is often called "cloud computing." 5 billion photos were hosted on Flickr as of September 2010. 2 billion videos are watched on YouTube every day. Facebook alone has more than 518 million active users who

[8] "Introduction to Book Excerpt: *The Numerati* by Stephen Baker," *Businessweek*, Aug. 28, 2008. Ironically, the 2008 story is actually referring to a January 23, 2006, cover story, "Math Will Rock Your World."

upload more than 20 million videos and spend more than 700 billion minutes on Facebook every month. 25 billion Tweets were posted on Twitter in 2010.

"Today, our biographies are etched in the ones and zeros we leave behind in daily digital transactions,"[9] Stanford Law School Professor and former dean Kathleen Sullivan has written. Personal digital data increasingly describe and define our lives, and those data, according to Marc Rotenberg, are "recording [our] preferences, hopes, worries and fears."[10]

At the same time, demand for personal data from business, the government, and other organizations is escalating. Access to personal data facilitates increasingly targeted products, services, and advertising. It makes possible greater user convenience, efficiency, and recognition. Personal information is regarded as increasingly essential to security and accountability.

Moreover, technology has not only contributed to an explosion in the ubiquity of data, but also the range of parties with physical access to those data, and the practical and economic ability of those parties to collect, store, share, and use those digital footprints. For example, in a credit or debit card transaction, the data are collected by the retailer, the transaction processor, the card issuer, the cardholder's bank, and the merchant's bank. Digital networks have also facilitated the growth of vigorous outsourcing markets, so information provided to one company is increasingly likely to be processed by a separate institution. Records containing personal data are linked and shared more widely and stored far longer than ever before, often without the individual consumer's knowledge or consent.

George Washington University Law School Professor Daniel Solove writes: "We are becoming a society of records, and these records are not held by us, but by third parties."[11]

Privacy Principles for the 21st Century

In the face of such dramatic changes since the OECD Guidelines were adopted 31 years ago, it is not surprising that they might require updating. While one is hesitant to tinker with principles that have undergirded all modern data protection laws, the focus of the Guidelines on discreet information exchanges seems outdated in a world of ubiquitous data flows. It is unclear whether individuals and data processors ever struck informed bargains over what data were being collected, for what purposes, and under what conditions, but that model appears so out of touch with today's reality as to require revision.

Fortunately, the careful wording of the Guidelines and the far-sightedness of their drafters allow for updating with minor, but important, revisions. These proposed changes serve the Guidelines' goal of protecting privacy without stifling innovation or expression and of "ensur[ing] that transborder flows of personal data . . . are uninterrupted and secure" and that data protection regimes are "simple and compatible."[12]

Here is one starting place:

---

[9] Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 128, 131 (2003).

[10] Louise Story, "To Aim Ads, Web is Keeping Closer Eye on What You Click," *New York Times*, Mar. 10, 2008, at A1.

[11] Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1089 (2002).

[12] O.E.C.D. , supra at ¶¶ 16, 20.

1. Collection Limitation Principle—~~There should be limits to the collection of personal data and any such d~~Data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Data should not be collected in a manner likely to cause unjustified harm to the individual unless required by law. "Harm" may include more than physical injury or financial loss. Harm is "unjustified" if caused by unfair or unlawful collection or use of data, or by processing in violation of the Data Quality Principle.

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.

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.~~ Organizations should collect and store data only as necessary to serve lawful purposes, and should make information about those purposes readily available.

4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used:
   a. for purposes likely to cause unjustified harm to the individual; or
   b. over the well-founded objection of the individual, unless necessary to serve an over-riding public interest,

   unless required by law. ~~other than those specified in accordance with [the Purpose Specification Principle] except:~~
   ~~a. with the consent of the data subject; or~~
   ~~b. by the authority of law.~~

5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle—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.

7. Individual Participation Principle—An individual should have the right with regard to data concerning, or used in a manner affecting, employment, health care, financial matters, or legally protected rights:
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above, and should be liable for the reasonably foreseeable harm caused by his failure to do so. Enforcement of data protection laws should achieve effective compliance with these principles and applicable law, while minimizing the burden on individuals or lawful information flows.

These changes are designed to serve specific goals that take into account the demonstrated success of the Guidelines, the significant changes in information technologies and applications over the past three decades, and the exceptional importance of privacy in an information age.

First, they respond to the reality that consent is an unworkable basis for most data processing activities and provides poor protection for privacy.[13] Second, they seek to impose an obligation that the collection and use of data be fair, lawful, and unlikely to cause harm—irrespective of whether or not there is consent. Third, they recognize that harm is a broader concept than just physical injury or financial loss. Fourth, they acknowledge that harm may be justifiable (for example, if a criminal suspect is apprehended on the basis of accurate, lawfully obtained information). What makes a harm unjustifiable is if the data are not collected or used fairly and otherwise lawfully, if the data are inaccurate, or if they are linked to the wrong person.

Fifth, the proposed changes to the Guidelines recognize that a well-founded objection to a use of data may be sufficient to block the intended use, but that such an objection may be overcome by an over-riding public interest. Sixth, the suggested language recognizes that the full range of individual participation rights should only apply where data concern, or are being used in a manner affecting, important matters or rights. Extending this principle to other data or other settings would in many cases be impossible given the way in which data are collected and stored, and could reasonably be anticipated to impose significant costs without yielding commensurate benefits. Finally, these changes seek to move beyond a mere compliance model to a broader understanding of accountability, in which organizations are stewards of the personal data that they collect, store, or use, and should be liable for the reasonably foreseeable harms that their failure to adhere to these principles causes.

The suggested changes otherwise leave the balance of the Guidelines unaltered. Security and transparency remain vital, along with the Guidelines' focus on flexibility, proportionality, and consistency across jurisdictions.

The language of the original Guidelines was carefully negotiated to address a variety of issues and cultural norms. Moreover, the Guidelines are supplemented by valuable commentary that provides additional details and guidance as to the drafters' intentions. The care with which the Guidelines and the commentary were drafted undoubtedly helps explain why the Guidelines have proved so influential and so durable. Any changes should certainly undergo similar scrutiny and discussion, and should be accompanied by appropriate commentary as well. The purpose here, therefore, is not to be overly focused on the actual wording of specific changes, but rather to indicate the types of changes necessary if the Guidelines are to retain their relevance in the 21st century.

[13] See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, Dec. 2010, 19-21, 25-28, available at www.ftc.gov/os/2010/12/101201privacyreport.pdf.