
THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

June 14, 2010

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

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams:

The Centre for Information Leadership (“the Centre”) appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration’s Notice of Inquiry, “Information Privacy and Innovation in the Internet Economy.” The Centre commends the Department for conducting this inquiry and for the important work it has undertaken to address this critical issue.

The Centre’s mission is development of sound 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 developing economies, and government use of private-sector data. The Centre has worked extensively with Asia Pacific Economic Cooperation (“APEC”) and the Organization for Economic Cooperation and Development (“OECD”) on issues of privacy and data protection. The Centre currently serves as secretariat for an international group of experts representing privacy protection agencies, civil society, academia and business that is exploring an accountability model for privacy governance.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. The Centre is located within the law firm of Hunton & Williams and is financially supported by approximately 40 companies. 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. However, the organizations listed at the end of this submission have expressed their support for the Centre’s recommendations contained herein.

In its response to this inquiry, the Centre offers ten recommendations and attaches supporting documents.

Centre Recommendations

1. The Department of Commerce should represent the United States in global privacy discussions.

The Department of Commerce must play a lead role in representing US interests in international discussions on privacy and global data flows. Over the past decade the US the Department of Homeland Security and the Federal Trade Commission have served in that capacity. Both agencies have their appropriate role, and the Federal Trade Commission has been recognized as best qualified for accreditation to participate in international conferences of data privacy commissioners. However, the Department of Commerce is best positioned to develop and advocate for US policy that fosters economic growth; robust, innovative use of data; and protection of privacy in forums where issues related to privacy are cross-cutting with issues related to trade, outsourcing, innovation, and technology policy. The Department of Commerce has played this role effectively in the past, for example in its work at the OECD and on the EU-US Safe Harbor, and continues to do so at APEC. We urge the Department to lead engagement in other international multilateral forums and in bilateral negotiations.

The Department of Commerce should seek out our trading partners' knowledgeable, effective representatives to ensure that the appropriate privacy and data protection models are considered. It must continue conversations with data protection authorities, but also broaden those discussions to include experts in trade, industry and specialized fields such as pharmaceutical research, to ensure that policies reflect sound, creative thinking about innovation, the importance of robust global flows of data to trade and economic growth, and respect for privacy.

2. The Department of Commerce should continue to support development of policy frameworks that will support the global flow of data.

The Department of Commerce must continue to promote global policy frameworks that ensure the robust, accountable flow of data. The Centre believes that the Department's experience in negotiating the Safe Harbor with the European Commission and in its role in developing the APEC Privacy Framework should be brought to bear to eventually

create a global framework that facilitates the flexible, accountable flow of data. These frameworks work best when based on agreed-upon, common objectives for data protection. The Department of Commerce should lead stakeholders in a process to develop those common objectives.

3. The government should articulate a vision for innovation and privacy in the information economy.

The Department of Commerce must articulate a unified vision for an innovative, safe digital environment that serves an information-driven economy. Such a vision must reflect both benefits derived from the business innovation that is driven by data, including personal data, and the responsible protection and management of information. Privacy must be positioned within that overall vision, and innovative uses of information must be compatible with data practices that promote privacy.

4. Information policy must have a home within the government.

The executive branch must demonstrate ongoing support for this vision by establishing a non-regulatory office that coordinates information policy in the United States. The information policy office must be led and staffed by experts who understand the technology, economic interests and societal values at issue as new business models and data applications evolve. Its role should include reporting on the advantages and costs to innovation of privacy protection. This office could be situated within the Department of Commerce. While the Centre does not believe this office should have a regulatory role, the agency should coordinate with the regulatory bodies charged with oversight and enforcing private-sector laws on privacy, information security and cyber security. The agency should also coordinate with the Privacy and Civil Liberties Oversight Board, which has similar responsibilities related to the government's use of information.

5. Both industry and government must be accountable for its use of information.

To be innovative, organizations must be able to explore data to understand its predictive value. Today, almost all business processes begin with the question "what does the data tell us?" To encourage growth through innovative information use, industry must be empowered to explore and use data robustly and responsibly.

The flexibility to be innovative must be conditioned on the organization's accountability for the manner in which it uses, manages and protects data. Every use of information

affects privacy. To strike the appropriate balance between the value created by data use and the risk that use poses to privacy, organizations must implement privacy processes that are as dynamic as their business processes. To be successful, the innovative organization must understand the privacy risks to individuals associated with the innovative use, and stand ready to mitigate those risks.

The assumption of the responsibility for the risks associated with innovative data use, and the willingness to be responsible for those risks form the basis of an accountability approach to data protection.

The Centre, through its Galway Accountability Project, defined the five essential elements of accountability:

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

Accountable organizations are responsible and answerable for the decisions they make about the use, management and protection of data. Accountability requires organizations to understand the risks they create for individuals by collecting and using information, and to mitigate those risks. In an environment where meaningful notice and choice become increasingly difficult to provide and exercise, accountable organizations make careful, balanced decisions about data, whether or not the individual has had an opportunity to make a choice about the use of his or her data. Accountability places the onus on organizations to be responsible about data, and relieves the individual of the burden of policing the marketplace against bad actors and

¹ The essential elements of accountability are more fully discussed in "Data Protection Accountability: The Essential Elements," October 2009, attached as Appendix A and found at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf> (last visited June 2, 2010).

making choices about data that may, in the end, provide little consumer control or protection.²

In recent months, accountability has figured prominently in discussions about how to improve privacy and data protection.³ Companies and policymakers are exploring how an accountability model for data protection might work in practice. What this inquiry has made clear is that accountability can only be effective for the private sector if government builds accountability into its information processes as well. The risk assessment and mitigation that lie at the heart of an accountability model must be adopted by government. While calls for such reform will likely be met with resistance, the private sector cannot be fully accountable if the federal government is not held similar requirements about the use and protection of data.⁴

6. Federal privacy law must pre-empt state laws.

U.S. business has repeatedly asserted that the “patchwork” of different, and often conflicting, state privacy laws impose significant burdens on companies that rely on data and data processing to run their business and power their product and service offerings. While many state legislatures have adopted innovative, effective approaches to privacy and security legislation, the nature of data use and data flows requires consistent, clear privacy law. Any federal privacy law should pre-empt state privacy laws from imposing requirements over and above those in federal legislation.

² The Safeguards Rule of the Gramm-Leach-Bliley Act provides an example of accountability that has worked well: the rule requires that companies secure their data, but leave decisions about how best to do so to the organization.

³ Discussion held during the recent series of Federal Trade Commission Roundtables entitled “Exploring Privacy” repeatedly identified accountability as an approach to data governance in a world of increasingly complex data uses and flows. At the Asia Pacific Economic Cooperation forum, models for implementation of the APEC Privacy Framework depend upon accountability to facilitate protected cross-border data flows. “The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data” notes the significance and utility of the accountability principle. 02356/09/EN WP 168, December 1, 2009, published January 11, 2010, by the Article 29 Working Party. Attached as Appendix B and available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf (last visited June 2, 2010).

⁴ A complete discussion of accountability can be found in “Data Protection Accountability: The Essential Elements; A Document for Discussion,” Attached as Appendix A and available at <http://www.ftc.gov/os/comments/privacyproundtable/544506-00059.pdf> (last visited May 27, 2010).

7. U.S. privacy policy should focus on successful privacy results rather than on procedures that do little to enhance privacy.

The US should avoid placing procedural requirements before strategic management of information and privacy protection. A checklist approach to privacy often results in a completed checklist rather than enhance privacy. Furthermore, the resources required to comply with procedural requirements often reduce those available to manage the real privacy risks to individuals. Some jurisdictions, for example, require companies to register all databases and notify officials if the data is to be processed in a manner different from that asserted, creating significant work for lawyers but providing little protection for individuals. In the U.S., advocates, experts and businesses have repeatedly commented that the annual privacy notices required by the Gramm-Leach-Bliley Act (but reportedly read by few consumers) have done little to promote privacy. In both cases, resources invested in complying with legal requirements would be better spent on initiatives that yield appreciable privacy results.

Alternative, comprehensive approaches to data management require that considerations and requirements for privacy, information security, and cyber security (as well as protection of intellectual property, trade secrets and evidentiary data) be part of an organization's overall data collection, storage, use and retention strategy. Governance approaches such as privacy by design, combined with accountability offer more effective information policy governance.⁵

8. Preventing harm must remain a significant feature of the U.S. approach to privacy.

Prevention of harm has been a feature of US privacy law since the enactment of the Fair Credit Reporting Act. Prevention of harm is a fundamental principle of the APEC Privacy Framework that supports setting priorities about data protection and enforcement based on the extent to which data practices may expose individuals to potential harm. The harm-based approach to privacy protection has come under criticism as focusing exclusively on financial and physical harm. But the potential for harm extends beyond the physical and financial to include the negative social impact harm to reputation, for example — that can result from the misuse of data. All three kinds of harm – physical, financial and social – should form the basis for setting protection and enforcement

⁵ Cavoukian, A., Abrams, M. and Taylor, S., "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," Office of the Information Privacy Commissioner, Ontario, November 2009, attached as Appendix C, and found at http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf (last visited June 2, 2010).

priorities. It will be important to carefully define the contours of social harm to provide businesses with a clear sense of their responsibility and the limits of their liability for such harm.⁶

9. The Department of Commerce should undertake an initiative to develop privacy norms that apply to data analytics.

Data analytics drive market innovation but also raise risks to individual privacy. Current data privacy guidance does not anticipate the power and speed of data analytics. The Centre urges the Department of Commerce to lead a process to set norms for analytics that encourage innovation, but create baseline guidance about their use in a manner that respects individual privacy. In developing those norms, it will be necessary to bear in mind the distinct differences in attitudes toward analytics that exist between the United States and its trading partners. Moreover, it will be important to recognize that no bright line has been identified between what information about an individual's behavior is and is not private.

Information and the ability to subject data to intensive analysis are essential to innovation and economic growth. With the freedom to understand the data comes the responsibility to use information in a judicious, disciplined fashion.

10. Privacy oversight and enforcement are best carried out by regulatory agencies with authority over specified industry sectors.

Any approach to privacy governance should preserve the current system whereby privacy is overseen by an industry sector's existing regulatory agency. Under such a model privacy enforcement benefits from the agency's intimate understanding of the challenges and opportunities companies face, the new business models and technologies companies adopt, the ways in which data is used and raises risks to privacy, and the overarching regulatory structure that governs the industry and that may impact the effectiveness of regulation or guidance and the opportunity for innovation and growth. Maintaining this system would preserve the value derived from familiarity with the way privacy governance works within an industry sector and within individual companies. In keeping with this model, the Federal Trade Commission should continue to oversee consumer privacy protection in general. As noted in Recommendation 3 of this submission, the Centre does not recommend creation of a

⁶ While notions of physical and financial harm are well established, the concept of social harm requires further exploration and definition. Such an inquiry is beyond the scope of this submission.

single privacy regulator, however it does believe there is a role for an office that would coordinate privacy, information security and privacy security policy in the private sector. That office would work with regulatory bodies to ensure that new technologies and business processes are reviewed and understood, and that policy guidance is applied consistently and appropriately across all sectors.

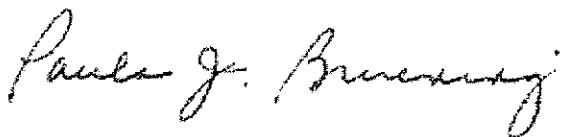
CONCLUSION

The Centre appreciates this opportunity to participate in the Department of Commerce's work to encourage data-driven innovation and effective privacy protection for individuals. 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 recommendation 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