Department of Commerce at the Intersection of Privacy and Innovation

June 25, 2010

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

1. Department of Commerce Should Take Lead Role as Global Privacy Advocate

This policy post is drawn from comments CDT filed in response to a Notice of Inquiry released by the Department of Commerce's ("DoC") Internet Policy Task Force ("Task Force") regarding the connection between privacy and innovation and the role the department should have in promoting online privacy.
The Commerce Department can support the global digital economy by supporting a comprehensive privacy plan in the U.S and supporting consumer trust as an innovation greenhouse.

Our comments ask the DoC to reaffirm that consumers' trust in the security and privacy of online transactions is a major reason for American business success. Commerce can advocate for American business by supporting sound user privacy policies and practices. In calling for the DoC to take a global leadership role on privacy, CDT emphasized that leadership begins at home.

CDT Comments [1] to the DoC NTIA Internet Policy Task Force: In the Matter of Information Privacy and Innovation in the Internet Economy [1]

A. Fair Information Privacy Principles

CDT believes that the DoC can play an important role in defining and clarifying privacy protections for consumers. We urged the department to endorse a modern, comprehensive set of Fair Information Practice principles ("FIPs") and to recommend that these principles be incorporated into a new baseline federal privacy law, executive branch policies, and self-regulatory guidelines.

The adoption of a baseline federal privacy law founded on FIP principles would have a global impact. Many international privacy frameworks, including the OECD guidelines of 1980, the Council of Europe data privacy convention, the EU Data Protection Directive, and the Asia-Pacific Economic Cooperation Privacy Framework, are all built around variations of the FIPs. Adoption of a U.S. law built around the FIPs would help U.S. companies adequately respond to differing legal regimes and empower the U.S. to assert global leadership on privacy.

The Department of Homeland Security's FIP principles – a modern and comprehensive set of FIPS [2]

2. Commerce Should Push for 21st Century Federal Privacy Protections

A. Support Baseline Consumer Privacy Legislation

The Task Force sought comment on the effectiveness of the current sectoral privacy framework, which CDT believes is insufficient to protect consumers and promote innovation in the 21st century. The current confusing patchwork of privacy standards differs depending on the type of data and the data collector. CDT believes that simple, flexible baseline privacy legislation that codifies a robust set of FIPs would protect consumers from inappropriate collection and use of their personal information, while enabling legitimate business. Baseline legislation should not preempt the strong,

sectoral laws that already provide important protections to Americans.

The comments highlight the potential interactions between a comprehensive federal privacy law and state privacy laws. States have been a critical laboratory for privacy innovation and experimentation; data breach laws are one of many examples of the important new ideas that have arisen from the states. But compliance with fifty different state privacy regimes can be burdensome for businesses, especially small or medium-sized entities or startups. For that reason, CDT urged the DoC to support the enactment of a comprehensive federal privacy with preemption that is narrowly tailored. Federal privacy law should not preempt state law unless it provides as much protection as the best state laws and expressly covers the same set of covered entities and same set of requirements.

In our comments, CDT also emphasized that policies that promote consumer privacy should be written so they will not impede the growth of small and medium sized entities (SMEs) and startups. Exceptions can be made for companies that handle small amounts of non-sensitive consumer data. CDT also called on the Commerce Department to recognize the potential burden that federal data retention laws would represent to SMEs and startup companies. Such laws could plausibly require online service providers to retain vast quantities of data for law enforcement purposes, damaging SME’s bottom line.

CDT comments on the 2010 Staff Discussion Draft Consumer Privacy Legislation [3]

B. The DoC should support ECPA reform

CDT's comments urged the DOC to consider the impact of current government access laws on individual privacy and technology innovation. Technology innovation has far outstripped legal protections for personal data in the United States provided by the Electronic Communications Privacy Act (ECPA). While ECPA was a forward-looking statute when enacted in 1986, it has not undergone a significant revision since then. ECPA is now an array of confusing standards that do not clearly apply to many new technologies. Inconsistent interpretations of the law by the courts have put both service providers and law enforcement agencies and putting user privacy at risk.

The outdated and overcomplicated privacy protections in ECPA can have a direct impact on the bottom line of the digital communications industry. Cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to permissive U.S. laws giving the government access to huge quantities of information with little judicial oversight. Consumers consistently cite privacy from government as a top concern when it comes to adopting cloud computing and location based services.

Without stronger legal privacy protection, the reluctance of consumers and businesses to use U.S.-based communications services may cause American companies to miss out on the jobs that would accompany new growth. CDT's comments recommended a detailed set of reforms to ECPA that would clarify existing law and offer privacy protections that reflect consumer expectations, but preserve the government's ability to get information when necessary. The CDT-led Digital Due Process coalition filed separate comments also focusing on reforming ECPA to protect consumers and reduce unnecessary costs on businesses.

Comments of the Digital Due Process Coalition: In the Matter of Information Privacy and Innovation in the Internet Economy [4]

Testimony of Jim Dempsey before the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties: ECPA Reform [5]

---

3. Commerce Should Re-affirm Intermediaries Are Not Liable for Privacy Violations

The Task Force requested input on the intersection of foreign and domestic privacy laws and the challenges these laws pose to U.S. businesses with global operations. CDT’s comments noted with concern cases where Internet intermediaries such as Web 2.0 platforms have been held liable for privacy violations in user-generated content. CDT believes that protecting technological intermediaries against liability for the conduct of their users has been critical in fostering growth and

innovation in technology industry.

In Europe, the question of liability for Internet intermediaries has arisen due to the unsettled interaction between the EU Electronic Commerce Directive (ECD) and the Data Protection Directive (DPD). Web 2.0 platforms have been held liable for privacy violations in user-generated content under the DPD, even as the ECD purports to protect them from liability. In our comments, CDT called on the DoC to bring together stakeholders from both sides of the Atlantic to discuss the negative implications of such inconsistency and to find common ground, both in Europe and abroad.

CDT also recommended that the DoC reaffirm the importance of protecting intermediaries from liability and seek to globally promote strong protections for intermediaries. The DoC should also seek to document the positive relationship between protecting intermediaries and fostering innovation. Tracking best practices for protecting privacy and serving other societal objectives in the context of user-generated content will help the DoC urge its counterparts around the globe to adopt laws that protect Internet intermediaries from liability for content posted by third parties.

CDT Paper: Intermediary Liability: Protecting Internet Platforms for Expression and Innovation [6]

4. Business Practices Should Be Consistent with Privacy by Design Principles

The Task Force requested information about the impact of privacy enhancing technologies and information management processes on business practices and consumers' experiences. CDT believes that all companies should implement the principles of Privacy by Design, a concept that offers a roadmap for integrating privacy considerations into business models, product development cycle, and new technologies.

CDT also urged the DoC to actively work to incentivize a robust marketplace of identity management products for consumers, as well as encourage government adoption of identity services that meet an established minimum standard for privacy. The DoC should explore the applicability of the Fair Credit Reporting Act (FCRA) to identity providers and investigate the potential of an FDIC-like regime for encouraging good practices amongst identity providers. CDT also suggested that the DoC, in conjunction with NIST, draft general best practices for identity management services and for their implementation by government and businesses.

CDT Consumer Privacy Roundtable Comments: The Role of Privacy by Design in Protecting Consumer Privacy [7]

CDT Consumer Privacy Roundtable Comments: Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers [8]

CDT Paper: Issues For Responsible User-centric Identity [9]

Source URL: https://www.cdt.org/policy/department-commerce-intersection-privacy-and-innovation

Links:
[1] http://www.cdt.org/comments/comments-cdt-department-commerce-information-privacy
[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[3] http://www.cdt.org/comments/cdt-comments-staff-discussion-draft-consumer-privacy-legislation
[4] http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf
[5] http://www.cdt.org/testimony/testimony-jim-dempsey-ecpa-reform
[6] http://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation
[7] http://www.cdt.org/content/role-privacy-design-protecting-consumer-privacy

[8] http://www.cdt.org/files/pdfs/CDT%203rd%20Privacy%20Roundtable%20Comments%20-%20Protecting%20Privacy%20in%20Online%20Identity.pdf
[9] http://www.cdt.org/paper/issues-responsible-user-centric-identity