ReedSmith

Commerce Privacy Green Paper Released, But It's No Second Fiddle to the FTC

Author: Amy S. Mushahwar, Associate, Washington, D.C

Publication Date: December 20, 2010

Paper Encourages FIPPs-Based Privacy Standard, 'Voluntary But Enforceable' Industry Codes, and the Creation of A New Privacy Policy Office

On December 16, 2010, the Department of Commerce's Internet Policy Task Force[1] released a privacy green paper entitled, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper"), which lends another voice to the privacy debate and attempts to create a universal privacy baseline. While the report makes no recommendations to cover specific industry sectors that are addressed by existing privacy regulations, such as health care, financial services and education, it is clear that the Department of Commerce would like to lead the regulatory agenda in the online privacy overhaul that is expected in 2011. In general, the release will kick start an ongoing discussion of privacy and we encourage organizations to undertake some cost-benefit analysis now for the best outcome in 2011.

Like the Federal Trade Commission's ("FTC") report (also see our blog post summarizing the FTC's Report) this Green Paper opens the beginning of an ongoing regulatory dialogue. In doing so, the Green Paper sets a decidedly different tone from the FTC's release just two weeks ago. Commerce invites far more reliance on cooperative industry self regulation, while proposing the creation of a Privacy Policy Office (PPO) within the Commerce Department that could coordinate the Administration's privacy policies in the United States and internationally. Functionally, the PPO would rest in the Department of Commerce (which would be more responsive to the Administration), rather than in the FTC (an independent regulatory agency that is subject to considerable oversight by Congress and is poised to change hands in January).

Basis: Consumer Trust in Data Collection Practices is a Necessary Predicate to Sustained Internet Innovation in the Global Community

The Green Paper recognizes that the Internet, as a medium, passed its teenage angst period, and developed into a medium of central importance to the domestic economy and global competitiveness.[2] To continue the medium's upward trajectory, Commerce identifies that consumers must feel confident to transact online. The Green Paper, like the FTC's Report, starts from the premise that consumers don't read privacy policies, don't understand privacy policies, and generally feel nervous that their information is being shared in ways they don't understand, despite the considerable efforts by industry to comply with existing law. Through its Green Paper, Commerce develops a roadmap to retool data privacy in the United States to facilitate domestic consumer trust and reinvigorate trust in U.S. data privacy practices, internationally. Its roadmap consists of the following themes:

- Keep the U.S. sector-specific framework, but fill in the "gaps" that are not addressed by the existing regulations
- Use the commitment to comprehensive Fair Information Practice Principles ("FIPPS" or, as it has been termed by the press, "a Data Bill of Rights") to establish a basis for greater interoperability between U.S. and international commercial privacy frameworks
- Foster the development of "voluntary but enforceable" industry codes of conduct that are more likely to adapt to the pace of innovation
- Create a new Privacy Policy Office (PPO) within the Department of Commerce that operates, without enforcement power, as the nexus of privacy policy
- Consider a national standard for security breach notifications involving personally identifiable information with some room for state enforcement and/or future legal nuance

10 Policy Recommendations with Implementation Questions To Focus the Privacy Framework Discussion

Each of the objectives identified above was translated into 10 more concrete policy recommendations that are identified below. The policy recommendations were accompanied

with corresponding questions for comment that were also published separately in a Federal Register Notice.

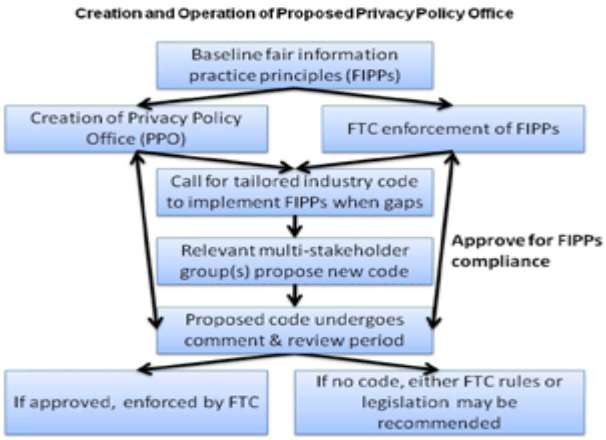
Recommendation #1, FIPPs: Any business outside the sector-specific framework would be subject to a baseline of Fair Information Practice Principles. The Green Paper identifies some potential FIPPs that are currently used by the Department of Homeland Security: transparency, individual choice, data purpose specification, data use limitations, data minimization with retention limits, data accuracy (data hygiene), security, accountability, training and auditing. Like the FTC Report, the Commerce Green Paper does not focus on whether consent should be "opt-in" or "opt-out"; rather, that the consent be obtained (or denied) after an effective consumer digital literacy campaign designed to facilitate understanding. Commerce seeks comments on the appropriate means to create the FIPPs. For example, would they be created by voluntary industry codes, by legislation, under Executive Order, or through FTC expanded rulemaking authority? Commerce also seeks comment on how the FIPPs would be enforced, such as, would the FIPPs be subject to consumer class actions?

Recommendation #2, Transparency, Use Limitations, Purpose Specifications and Audits: The Green Paper calls for a "high priority" focus on transparency, identifying that companies need to go beyond the obvious of simplifying and shortening policies. Understandable data purpose specifications should be added to policies, along with use limitations on how the data should be shared and disclosed. Commerce briefly mentioned that technology, such as a "Do Not Track" mechanism, could hold some promise for simplifying notice and choice, but there is no industry consensus on the human-to-technology interaction. Instead, Commerce highlighted for comment the idea that Privacy Impact Assessments (PIAs) could be used in the private sector to provide detailed evaluations of the privacy protections in place for the data flows collected by new products and services.[3] Commerce also recommended that data auditing (which the Green Paper does not identify by whom or recognize the myriad existing privacy sector data audits) could verify if companies are abiding by their use limitations.

Recommendation #3, Adaptable "Voluntary But Enforceable" Industry Codes for New Issues and Technology Outside the FIPPs: Commerce summarized concerns that the FIPPs may, at times, be vague as to applicability, grow outdated, or lack sufficient certainty to guide compliance. To guide industry implementation, Commerce would like to foster the development

of flexible industry codes through a multi-stakeholder process. Commerce suggests that it could safe harbor companies that adhere to the codes to provide incentive for their creation.

Recommendation #4, Establishment of a Privacy Policy Office (PPO) within NTIA: The Green Paper proposes the creation of a PPO within NTIA, the executive branch agency principally responsible for advising the President on telecommunications and information policy. The PPO would coordinate the development of industry codes in the United States and represent U.S. data policy abroad. The PPO would also assist with consumer education campaigns (it bears mentioning that NTIA initially started the digital television transition consumer campaigns with mixed reviews). The new PPO would not have enforcement authority; rather, it would be a forum for discussion and the expedient development of voluntary standards that may be more responsive than the rulemaking process. Commerce provided the following diagram to illustrate the role of the PPO:



Commerce seeks comments on the appropriate "carrots and sticks" to encourage the development of industry codes.

Recommendation #5, Keep the FTC as the Enforcement Lead. Commerce recommends that the FTC keep its role as the enforcer of consumer privacy. However, many issues regarding the appropriate role and authority of the FTC are open for comment, such as: Would the FTC need further rulemaking authority to elaborate on the FIPPs? Or, would it need specific legislative authority for its enforcement role?

Recommendation #6, Transborder Data Flow (with an Eye on the Tiger). Commerce would like the United States to take a leadership role in creating international data transfer frameworks to reduce the current compliance headaches that are experienced by industry. Such frameworks could be established under mutually recognized privacy regimes (that could also be implemented in-country). In the near term, Commerce has its eye on the lucrative and populous Asian market. Its goal is to secure an endorsement from the Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder[4] and solidify a cross-border privacy rules system for the APEC region to transfer data to the United States. Ultimately, Commerce aims to continue this discussion globally to foster greater harmonization of privacy and security legal frameworks.

Recommendation #7, Consider a National Security Breach Notification Law. Commerce would like to pull concepts from existing state breach law (and the lessons learned from breaches under those laws) to fashion a national standard. Any proposal would continue to encourage companies to maintain high security standards (and Commerce has raised the possibility that states could develop more restrictive law than the national standard). Such a national standard would not displace any existing sector specific breach standard (e.g., HIPAA, GLB, CPNI and so on). Commerce has invited comments, however, on the threshold for notice under such a standard (e.g., harm or a specific threshold such as a number of records).

Recommendation #8, Sector-Specific Laws Stay, FIPPs Supplement. Commerce identified at the outset, and reiterated here, that it will not supplant existing sector-specific laws. Commerce also continues to reference "commercial data privacy policy," so its policies would also be inapplicable to non-commercial uses, such as government data.

Recommendation #9, Preemption, Perhaps? Commerce appears to steer clear from a definitive position on the tricky issue of state preemption. Instead, Commerce tees this issue up for comment. Commerce seeks guidance on: the appropriate degree of preemption, the ongoing need for consumer class actions and the potential for state attorneys general to enforce any national standard developed.

Recommendation #10, ECPA Reform: Commerce identifies the concerns of previous commenters that the Electronic Communications Privacy Act ("ECPA") lags behind and may create impediments to the further development of new technologies, such as cloud computing and location-based services. Commerce seeks further data substantiating the concerns that cloud computing could lead to ECPA violations as a result of the perceived insecurity of data in

the cloud. Commerce also seeks comment on the whether the current protections for transaction information and location information are adequate. Commerce additionally would like to hear from law enforcement about the impact of any proposed reforms to the investigation process.

Why is this Important?

The Commerce docket will kick start an ongoing discussion regarding the framework for regulation of privacy. Businesses that do not participate in the privacy discussions before the Department of Commerce and the Federal Trade Commission cannot cry foul if unfavorable data privacy and cyber security recommendations are implemented. We urge you not to suffer silently. Undertaking some cost-benefit analysis now to substantiate any concerns that your company many have could help preserve the value of your information assets or save your team some compliance headaches down the road.

Comments are due to the Department of Commerce on or before January 28, 2011.

Comments are also due to the Federal Trade Commission a few days later, on or before January 31, 2011.

---

1. The Internet Policy Task Force ("IPTF") includes government officials from the National Telecommunications and Information Administration ("NTIA"), the Patent and Trademark Office ("PTO"), the National Institute of Standards and Technology ("NIST"), and the International Trade Administration ("ITA"). As stated on the IPTF's website, it was convened to take a comprehensive review of the link between "privacy policy, copyright, global free flow of information, cybersecurity and innovation in the Internet economy." For more information, *see*: www.ntia.doc.gov/internetpolicytaskforce

2. Commerce identifies that global online transactions total an estimated $10 trillion annually and U.S. domestic online transactions are estimated to total $3.7 trillion.

3. PIAs are heavily used in the government context and they analyze how a specific product, database or system of record has incorporated privacy protections into its entire lifecycle. The PIA process itself requires organizations to think through the appropriate and timely handling of privacy concerns. Such a PIA proposal would be in keeping with

the FTC's Privacy by Design proposal. The concept of both PIAs and Privacy by Design is that potential privacy issues should be discussed, remediated (to the extent feasible) and disclosed to the consumer at the outset of the design process.

4. For further information on the Privacy Pathfinder project developed by APEC's Electronic Commerce Steering Group, see webapps.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.