THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP

A Comparison of the Recent FTC and Commerce Department Data Privacy Frameworks

By Lydia Parnes & Edward Holman

As the IAPP enters its second decade, the privacy landscape in the U.S. is undergoing a major revamping. Last December, the Federal Trade Commission (FTC) and the Department of Commerce (DoC) separately proposed new policy frameworks for analyzing data privacy. These proposals are the culmination of separate—and comprehensive—reviews conducted by the agencies over the past year. This article summarizes the two proposed frameworks, explores where they are similar and where they differ and suggests what impact these frameworks, if adopted, may have on businesses that collect, use or disclose information about consumers.

The FTC's report, entitled "Protecting Consumer Privacy in an Era of Consumer Change: A Proposed Framework for Businesses and Policymakers," was released on December 1, 2010, and proposes a privacy framework based upon three general principles: privacy by design, simplified choice and greater transparency. The DoC's green paper, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," was released two weeks later on December 16, 2010, and focuses on five topics: expanding Fair Information Practice Principles; promoting voluntary, enforceable privacy codes of conduct; encouraging global interoperability of privacy regimes; standardizing security breach notification rules, and revising the Electronic Communications Privacy Act.

The agencies agree on a number of topics, including giving consumers greater transparency into and choice regarding the collection and use of data about them. The agencies differ, however, in the scope of their reports and their positions on self-regulation. The FTC report is comprehensive in scope; proposes voluntary industry adoption of a do-not-track mechanism in the online context, and expresses some frustration with the delay in implementation of an industry self-regulatory program for online advertising. In contrast, the DoC report proposes the adoption of voluntary codes enforceable by the FTC as well as the creation of a Privacy Policy Office within the department. No matter the final outcome, these reports raise significant issues for both enterprises and privacy professionals.

Scope of Reports

At the outset, the FTC and DoC reports differ on their scope. The DoC proposes a framework that would apply to the online collection of data; the FTC proposal is strikingly broad and would apply to all commercial entities that collect or use consumer data, whether online or offline, that reasonably can be

linked to a specific consumer, computer or other device. With this broad scope, the FTC continues to move away from a distinction between "personally identifiable" and "non-personally identifiable" information.

Beyond Privacy Policies

The FTC and DoC reports indicate that both agencies want to move away from the existing model, where companies disclose their data collection and use practices in their privacy policies and the FTC enforces breaches or other unfair practices as violations of Section 5 of the FTC Act. The FTC, for example, believes that this model has resulted in enforcement that focused on a too limited range of consumer harms. The FTC proposes to address "the actual range of privacy-related harms [which] is much wider [than physical or economic harm] and includes reputational harm as well as the fear of being monitored or simply having private information 'out there.'" Similarly, the DoC noted that "[f]rom the consumer perspective, the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use..."

To supplement notice-and-choice, both agencies propose a number of preemptive data privacy protections. The FTC, for example, proposes that industry adopt a "privacy by design" approach, where privacy and security is built into everyday business practices. According to the FTC, data should only be collected for legitimate business purposes, used only for those purposes, retained only as long as necessary to serve those purposes and disposed of safely once no longer needed. In addition, businesses should implement procedures to ensure that the information they collect and retain is accurate.

The FTC also proposes that companies maintain comprehensive data management procedures throughout their product or service lifecycles. This would entail procedures such as designating specific personnel responsible for privacy issues, conducting periodic reviews of privacy policies in light of relevant developments and using privacy-enhancing technologies to establish and maintain strong privacy policies. The FTC advises companies to scale the size and scope of these programs to the risks presented to the data they collect, use and maintain.

Similar to the FTC's approach, the DoC makes several recommendations regarding Fair Information Practice Principles (FIPPs). The DoC recommends that an expanded set of FIPPs be used to establish a baseline commercial data privacy framework; these FIPPs would essentially be a guiding set of principles that would establish the minimum level of online privacy protection nationwide. Although the DoC does not propose a specific set of FIPPs, it does cite favorably principles adopted by the Department of Homeland Security, which include transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security and accountability and auditing. The DoC did not take a position on whether these FIPPs should be imposed by new legislation, but sought public comment on this topic.

Transparency and Consumer Choice

Both the FTC and the DoC agree on the importance of increasing the transparency of privacy practices for consumers. The FTC, for example, notes that privacy policies continue to play an important role in promoting transparency, accountability and competition on privacy issues, but only if they are clear, concise and easy to read. In particular, the report criticizes existing privacy disclosures for being both insufficient and too complex. As a solution, the FTC proposes that companies make privacy policies clearer, shorter and more uniform so that consumers, regulators and others may more easily compare policies among different companies.

To further promote transparency, the FTC proposes that companies offer consumers access to the data they hold about them. Of particular concern to the FTC are data brokers that combine consumer data from several sources and resell it, often without the consumer's knowledge. Recognizing the potential burden in providing access, the FTC supports a sliding-scale approach where the extent of access would depend on the sensitivity of data and its intended use.

Finally, the FTC proposes that companies obtain affirmative opt-in consent from consumers before using consumer data in a materially different manner than claimed when the data was collected. For example, the FTC proposes that social networking sites obtain opt-in consent before making previously private information public. Additionally, the FTC asks for increased consumer education and awareness regarding commercial privacy practices. This particular proposal seems to reflect agency guidance and enforcement policy in the recent past and a more definite statement on this particular issue.

Similar to the FTC's proposals, the DoC recommends that expanded FIPPs focus on greater transparency, more detailed purpose specifications and use limitations and auditing. Specifically, the DoC criticizes current privacy policies as being overly long, too complex and a generally poor method of conveying privacy information to consumers. In addition to advocating for simpler, clearer notices, the DoC looks favorably on privacy impact assessments, which require companies to identify and evaluate privacy risks, as a complementary approach to increasing transparency. Additionally, the DoC suggests using purpose specifications—which require companies to state the reasons they are collecting data—and use limitations—which require companies to use the data collected for only the stated reasons—to better align consumer expectations and actual data practices. Finally, the DoC argues that companies need to better audit their privacy practices to ensure that they are living up to their stated practices.

In addition to advocating for greater transparency, the FTC also proposes that companies provide choices to consumers in a simpler, more streamlined way than in the past, when businesses are utilizing information beyond "commonly accepted" practices. Under this approach, when companies engage in certain "commonly accepted" practices such as order fulfillment and internal operations, fraud prevention and legal compliance—practices consumers have come to expect—companies would not need to provide notice and choice to the consumer. Notably, the FTC includes "first-party" marketing as a commonly accepted practice that does not require consumer choice.

For most other practices, the FTC suggests notice and choice at the point of collection in a way that is clear, concise, easy-to-use and incorporates durable choice mechanisms. The FTC proposes that such choice be offered at a time and in a context in which a consumer is making a decision about his or her data. Furthermore, the FTC proposes that enhanced consent may be warranted in certain situations, such as where children, sensitive information or deep packet inspection are involved. While it is not clear from the report exactly what shape this enhanced consent will take, businesses should expect the agency to require some form of affirmative express consent—or even more heightened restrictions—in these situations.

Finally, the FTC suggests that consumers should be given better choices regarding the collection of information about them, not just the use of such information for direct marketing purposes. The FTC points favorably to a more uniform and comprehensive choice mechanism for online behavioral advertising, sometimes referred to as "do not track," as a means for exercising choice in the context of behavioral advertising data collection. A do-not-track mechanism would potentially function as a persistent Web browser setting that would inform Web sites of the consumer's privacy preferences.

Enforcement

The agencies differ on enforcement. To supplement FIPPs and provide a framework with more practicality and certainty, the DoC recommends the creation of voluntary, enforceable codes of conduct (CoCs). The DoC argues that these CoCs should focus on emerging technology issues not adequately covered by baseline FIPPs and points to the Network Advertising Initiative's CoC for behavioral advertising as an example. To promote the development and adoption of CoCs, the department suggests several possible approaches, including public statements of administration support, increased FTC enforcement and legislation that would provide a safe harbor for companies that comply with approved CoCs. To qualify for safe harbor status, the DoC states that these CoCs should undergo an open, multi-stakeholder process and be approved by the FTC.

The DoC also recommends creating a Privacy Policy Office (PPO) within the department. The purpose of the PPO would be to convene multi-stakeholder discussions of various information privacy issues, including industry CoCs. The PPO would not have any enforcement authority and would focus solely on commercial data privacy practices (as opposed to, for example, government practices). As currently proposed, the PPO would work with the FTC on policy issues such as do not track. It remains to be seen, however, whether the creation of the PPO would produce any material benefit, or if it would simply open the door to diverging policy views.

Finally, the DoC recommends that the FTC remain the lead consumer privacy enforcement agency for the U.S. government but suggests that there is room for additional or concurrent state enforcement of data privacy practices. Furthermore, the DoC suggests that any federal data privacy law not completely preempt state laws but leaves the degree of preemption and the extent of state enforcement open for public comment.

While the DoC may look favorably on self-regulatory activities as a means of implementing new, substantive privacy protections, the FTC, in its report, makes it quite clear that it feels differently. Specifically, the FTC criticizes industry efforts to self-regulate as too slow and having failed to provide meaningful protection for consumers. For its do-not-track proposal in particular, the FTC suggests that, absent voluntary industry adoption, legislation may be required for implementation. While both the FTC and the DoC cite industry efforts to provide consumers with behavioral advertising opt-out capabilities such as in-ad notice, the FTC feels these efforts have fallen short. Nevertheless, industry groups continue to push ahead on these initiatives, and companies should continue to participate in self-regulatory programs as a means of providing a better experience to consumers.

Promoting Legislative Clarity and Consistency

In addition to the recommendations above, the DoC makes several additional proposals to bring consistency to global and national privacy laws, an area not addressed by the FTC. First, the DoC advises the U.S. government to engage other global privacy enforcement authorities in developing a framework for mutual recognition of commercial data privacy systems. The lack of such a framework, the agency argues, is both costly and confusing. U.S. companies that operate across multiple jurisdictions are not only required to pay the cost of compliance in those different areas, but also must decipher what legal obligations arise as they transfer information across international borders.

The DoC believes the best way to address this problem is to create a system of cross-border privacy rules, preferably within the framework already established by the Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder project. As the 2011 APEC host, the agency believes that the U.S. is in a unique

position to promote acceptance of a self-regulatory system that would clarify the obligations and requirements on businesses seeking to transfer data between businesses stationed in APEC nations. The agency also believes that the implementation of a clear and understandable framework will encourage companies to act responsibly, as APEC will create a mechanism for enforcement if they do not.

Next, the DoC recommends that the U.S. establish a comprehensive commercial data security breach notification framework for electronic records. Under the agency's vision, this framework would serve as a national baseline; if states opt to build on that framework, they would be permitted to do so in limited ways. The agency suggests that guidance for this new framework be taken from the state systems that currently operate as the primary source of law in this area. Furthermore, the agency supports the implementation of a national framework to unify the minimal requirements for data security as well as the clarification of the requirements each business must undertake to protect the data in its possession. The agency's recommendation, however, only applies to current state security breach notification laws; it makes no recommendation regarding breach notification laws for specific sectors such as healthcare. The agency sought comment on what factors breach notification should be predicated upon.

Finally, the DoC recommends that congress reconsider existing legislation, particularly the Electronic Communications Privacy Act (ECPA), to ensure privacy protection in cloud computing and location-based services. The ECPA was enacted in 1985 to balance personal and proprietary privacy interests against the government's law enforcement needs. The agency suggests that the current state of information technology has outgrown the ECPA, leading to inconsistent interpretations of the law. The agency, therefore, seeks to rebalance the ECPA in light of new technologies and interests, with the aim of both protecting consumer expectations of privacy and effectively punishing unlawful access and disclosure. The agency sought comment on the most effective way to strike this balance.

Conclusion

While neither agency has announced when they will issue final versions of their reports, they are expected to be issued sometime later this year. Nevertheless, there are a number of issues that businesses will want to begin addressing now. First, given the scope of the FTC's report, businesses that collect, use or disclose information about consumers either online or offline—and regardless of whether that information is personally identifiable—may want to take a fresh look at their information practices. As a practical matter, businesses that have addressed data issues from the perspective that they do not collect personally identifiable information need to understand that this distinction is becoming increasingly less important.

Additionally, the proposals by both agencies that companies implement "baked-in" privacy protections are consistent with broader trends in this area but may particularly impact newer and emerging enterprises faced with limited resources for these kinds of efforts. Enterprises may want to think carefully—and earlier—about information governance strategy, especially where a business model depends upon or requires data monetization. If ultimately adopted, increasing levels of consumer control of data—and the need for accountability from and among data partners—seems highly likely.

With regard to giving consumers additional notice and choice, businesses that may not have recently reviewed their privacy policies or adopted such policies with a focus more directly upon personally identifiable information versus other information, may want to review and evaluate their policies—and more importantly the underlying practices—as a prudent risk management strategy. Furthermore, broad consumer access to data collected and held by business, as proposed by the FTC, may present particular

challenges for smaller and newer businesses, and represents an area for careful study by many enterprises. Companies should seriously consider participating in credible self-regulatory programs that address notice and choice issues now to help get ahead of regulatory enforcement in this area.

Both agencies sought public comment on a wide variety of issues raised by their respective reports. Because the comment deadline for the FTC's report was still pending as this article went to press, please look for a follow-up article summarizing issues raised by the filed comments in the next issue.

This article first appeared on March 1, 2011, in the Privacy Advisor *and is used with permission from the International Association of Privacy Professionals. Learn more at http://www.privacyassociation.org.*