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

A Summary of Comments Filed on the Recent FTC and Commerce Department Data Privacy Frameworks

By Lydia Parnes, Edward Holman, and Daniel Kane

In last month's edition of the *Privacy Advisor*, we compared the new policy frameworks for analyzing data privacy separately proposed by the Federal Trade Commission (FTC) and the Department of Commerce (DoC). In this issue, we summarize the comments that were submitted in response to each of the frameworks and examine some of the common issues addressed in the submissions.

The FTC Report

As a reminder, 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. At last count, the FTC had received well over 400 comments from a wide variety of parties, including individuals, corporations, academics, government agencies and various other organizations and interest groups representing both industry and consumers. Although the comments vary, many address similar themes, including the scope of the report, how to define "commonly accepted practices," Privacy by Design, allowing consumer access to data, industry self-regulation in behavioral advertising and Do Not Track.

Scope of the Report

The broad scope of the FTC report ("commercial entities that collect, maintain, share or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or other device") generated a significant reaction. Business and industry groups believe that the proposed scope is too broad and recommend that the FTC clarify its intended scope and identify exceptions or limitations. For example, several industry groups are concerned that the FTC's proposed framework will address practices that are already regulated by sectoral privacy laws such as the Fair Credit Reporting Act (FCRA). Industry groups, corporations, and some consumer groups propose at least some limitations for small organizations that only process a limited amount of non-sensitive information. Other proposed limitations by industry include exclusions for business-to-business communications and publicly available information. Some consumer groups and European government organizations, however, advocate for not limiting the scope.

One scope-related topic that receives a lot of attention in particular is the FTC's suggestion that the distinction between personally identifiable information (PII) and non-PII is blurring. Many commenters

support this proposition to varying degrees, though others point out that although the line may be blurring, the distinction has not vanished entirely. In particular, some companies and organizations are concerned that including information such as IP addresses and other identifiers essential to basic network functionality could have broad, unintended consequences. Thus, some commenters propose limiting data subject to regulation based on its sensitivity and context.

Commonly Accepted Practices

The FTC proposal would exempt "commonly accepted practices," such as product fulfillment, internal operations and fraud prevention, from a mandatory choice requirement. Some groups find the FTC's proposed definition to be too broad, others too narrow and others object to the concept entirely because they are concerned that any definition would be too rigid, thus inhibiting innovation and not accounting for shifting consumer preferences. One specific point of contention is the inclusion of first-party marketing as a commonly accepted practice, with companies and industry groups arguing that "third-parties" who act on behalf of "first-parties" for marketing purposes should be included within the exception, and some consumer groups and others arguing to the contrary. Others are concerned that certain commonly accepted practices proposed by the FTC, such as product improvement, may be used to justify a broad range of practices, or that vagueness with certain exceptions may lead to legal uncertainty. Finally, some industry groups argue that third-party data sharing is a commonly accepted practice due to widespread use, though some concede that choice should still be offered with respect to third-party marketing.

Privacy by Design

The Privacy by Design principle, which encourages developers to build privacy protections into applications from the outset, receives mostly positive comments in the submissions. Nevertheless, while many industry groups and companies express support for Privacy by Design as a best-practice principle, they also express concern that translating Privacy by Design into prescriptive rules could stifle innovation and impede new product development. Generally speaking, however, the submissions of many companies describe how they are already incorporating Privacy by Design principles in their operations and express support for the Privacy by Design concept.

Consumer Data Access

A number of companies and industry groups express concern about the proposal to allow consumers access to the data that companies have about them and the related principle of ensuring data accuracy. They believe that turning the privacy principles of data retention and accuracy into specific regulatory requirements may create undue burdens for businesses with little or no countervailing benefit. Some commenters argue that requiring the accuracy of consumer marketing data not already covered by privacy laws such as the FCRA will pose significant costs on businesses for data that is generally not used to make eligibility decisions. A number of commenters argue that the FCRA already provides data access and accuracy requirements where appropriate and thus broader requirements are not necessary. Additionally, some companies and industry groups are concerned that providing consumer access to data may not be feasible where third-party data aggregators have no direct relationship with consumers, thus raising authentication issues. Many parties agree that if data access is required, companies should be able to charge a reasonable fee for providing such access.

Industry Self-Regulation

Another hot topic addressed in the comments is the effectiveness of industry self-regulation, especially in the field of online advertising. In its report, the FTC is critical of industry efforts to regulate thus far, and many consumer advocacy groups echo this concern. The comments of many companies and industry groups, however, cite recent self-regulatory activity as a preferred alternative to government intervention. In particular, a number of companies and industry groups involved in the online behavioral advertising space tout the recent implementation of the industry's Self-Regulatory Principles for Online Behavioral Advertising in the form of an "Advertising Option Icon" that will appear on targeted online advertisements. This icon provides in-ad notice for behavioral advertisements participating in the program and provides consumers a method for opting out of data collection and/or use. The self-regulatory program includes enforcement of the industry's OBA principles by the Direct Marketing Association and the Council of Better Business Bureaus. Several commenters, however, express concern that the further adoption of industry self-regulatory activities is being threatened by the FTC's support of a Do Not Track mechanism. According to these commenters, the FTC should clarify its support of self-regulation and its position on Do Not Track. On the other hand, a number of consumer groups feel that the industry's opt-out implementation is insufficient for a number of reasons, including, they argue, that it is not universal, not persistent and that in many cases only stops data use—not collection. These groups thus argue that legislation will be the only truly effective means of providing meaningful privacy protections.

Do Not Track

Perhaps not surprisingly, the FTC's Do Not Track (DNT) proposal generated a significant reaction. In its report, the FTC urges Web browser developers to create and integrate a universal opt-out solution into their browsers. Subsequently, Congresswoman Jackie Speier has introduced legislation that would grant the FTC the power to define DNT rules. Most businesses that submitted comments generally believe that consumers should exert some control over the manner in which companies advertise to them. This does not mean, however, that these businesses support the imminent implementation of DNT legislation. As a preliminary concern, a number of commenters note that there is considerable confusion over what DNT covers. Some businesses believe that it applies only to interest-based or behavioral advertising; others view it much more broadly, applying to any online tracking. Rather than implement a program in this undefined area, commenters propose that the government focus instead on understanding fundamental consumer concerns of data collection, usage/sharing and obligations.

Commenters also note that, if implemented in its current manner, the proposed DNT legislation would drastically affect all general Internet functions. These commenters claim DNT would eliminate basic data collection necessary for routine Internet operations and severely limit the manner in which companies could monetize the online experience. For example, commenters claim that this new law would "break" businesses that aggregate or license content, create content or provide platforms for users to create their own content.

Some businesses believe that implementing a national DNT law at this time is premature; instead, they prefer to wait until consumers' expectations, wants and needs are better understood before taking action. They believe that, after further study, it will become apparent that each industry is different and that each entity should be able to offer a mechanism that best fits their business model or the needs of their users. If congress is set on passing legislation here, however, these commenters suggest that the new law follow the FTC's guidance. Under this proposal, data practices of entities that do not directly engage with users, and thus are not accountable to users, would not be covered. This

standard would create a contextual DNT approach that recognizes differences in user expectations and adopts bifurcated requirements for companies depending on whether they are known to and interact directly with users. Just as consumers have the right to tell telemarketers not to call them and to opt-out of e-mail solicitations, so should they have the right to opt out of online tracking when and if they wish to.

Many commenters also address the recent DNT implementations proposed by Google, Mozilla and Microsoft. Google's solution is an extension to its Chrome browser that preserves industry opt-out cookies even after a user clears all their cookies. Mozilla's solution is a header notice that is sent to Web sites indicating a user's opt-out preference. Microsoft's solution is a set of lists maintained by third parties that block tracking cookies from being set in Internet Explorer. Criticism and praise for each solution can be found throughout the comments, with the only real agreement being that there is no consensus on which implementation will provide the best solution.

The Department of Commerce Report

On December 16, 2010, the DoC issued its "green paper" on data privacy in the twenty-first century, titled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." One hundred businesses, trade groups and individuals submitted comments. Generally, these comments addressed two central issues: first, whether congress needs to enact legislation to establish baseline privacy protections and, if so, what form that legislation should take; and second, what type of policy guidance should DoC provide concerning information companies should be required to disclose to the public, and which agency should oversee any proposed regulations.

LEGISLATION

The Need for Legislation

A number of submissions begin by addressing the basic issue of whether congress should legislate to provide a national data retention policy framework. If congress were to act, the green paper suggested that it codify the Fair Information Practice Principles (FIPPs). Many businesses and trade groups oppose this idea; instead, they prefer continued reliance on self-regulation to ensure proper industry practices. Industry believes that self-regulation has been effective thus far in fostering consumer trust, securing consumer data and spurring innovation in the markets. It argues that the FIPPs were designed to be general and to serve as "guiding principles" to be applied relative to the context and data at issue. By instituting an official framework that all actors must follow, industry predicts that the resulting regime would be too inflexible to respond appropriately to the rapidly developing technological environment. This, in turn, would serve to seriously impede innovation. Even if implemented, many commenters believe that this legislation would be ineffective. The creation and implementation of law is a lengthy process; there is a significant likelihood that new issues not previously considered would arise after the law was enacted, thereby diminishing the legislation's scope.

Those who support a legislative solution claim that self-regulation is inadequate; businesses, they argue, are not restricted by self-regulation regimes because the parties who oversee these processes rarely have an incentive to materially punish offenders. Legislation proponents argue that, as the architects of these self-regulation systems, the industry participants who compose the review boards want only to achieve superficial results; they have minimal, if any, interest in protecting consumer rights or accomplishing long-term industry change. The consumer groups and companies that support this position believe that incorporating FIPPs into commercial data privacy legislation will provide

greater protection for consumer data and engender a greater level of confidence and trust in e-commerce. They believe that a legislated answer is the only way that consumers will ever trust businesses with their private commercial data. These commenters also argue that legislation will benefit those in the industry; by creating a clear and understandable framework, businesses will know for certain the types of data they can retain as well as understand the associated liability attendant to any violations of this policy.

Preemption

If congress does legislate, the question remains whether this new statute should preempt state laws. Those who favor preemption argue that any federal regulatory scheme would be undermined if every state could implement its own rules and regulations; they opine that federal preemption is necessary to maintain consistency. They note that even minor differences among state laws implementing FIPPs could present an undue burden on businesses that serve a multi-jurisdictional customer base without providing any substantive benefit to consumers. In support of this, they allude to the current patchwork of state commercial data privacy laws and regulations and note the resulting difficulties this has caused for many businesses, especially smaller businesses and entrepreneurs that participate in interstate commerce. Finally, these commenters argue that a federal law that provides for preemption of state laws governing the same subject matter would help ease the compliance burdens for companies attempting to track and comply with an ever-changing state law landscape regarding breach notification.

Those who oppose federal preemption do not object to the federal government acting in this area. Rather, they wish to preserve for the states the right to enact supplemental laws to provide citizens with a greater level of protection. These advocates, many of whom are consumer groups, believe that federal law should be considered a floor rather than ceiling. They note that citizens of different states have varying expectations regarding the manner in which their data is collected and that local governments should be empowered to meet heightened needs if they exist. In the event that the federal government deems preemption absolutely necessary, these groups advocate that it limit preemption to narrow categories and allow for most state laws in the area to remain untouched.

Safe Harbors

If congress enacts legislation, most commenters favor including a safe harbor provision to protect entities attempting to adhere to the new law. Under this plan, any safe harbor must provide the reviewing government agency with reasonable criteria to judge the acceptability of the contested actions while also encouraging innovation. To support the new law, these commenters require some assurances that the safe harbor will apply for a reasonable period of time and that it will not be overturned. They believe that the safe harbor should be designed to encourage further consumer engagement and transparency; it should, therefore, provide incentives for businesses to incorporate strong privacy principles into their practices and to describe their data practices fully in privacy policies and other notices.

Absent legislation, other commenters still believe that self-regulatory organizations should include safe harbor protections within their organizational charters. These parties note that acceptable practices within data collection and retention constantly change and that the development of a safe harbor would encourage the industry to develop and adopt self-governance practices that address emerging issues, and to follow such practices. In their opinion, providing a safe harbor for companies that adhere to a voluntary code of conduct will create incentives to develop such codes of conduct. A robust safe harbor would encourage companies to participate in self-regulatory efforts and would help

ensure the broad industry support that is necessary to ensure active enforcement of such codes. In their view, a safe harbor rewards companies that play by the rules and properly subjects those that do not to disciplinary action.

POLICY ISSUES

Privacy Impact Assessments

The commenters who discuss privacy impact assessments (PIAs) are nearly uniform in their belief that these reviews are useful and effective for the companies that conduct them. Generally, these commenters believe that the decision to conduct PIAs belongs with the company and that the government should not mandate them. If particular businesses want to publish their PIAs, this should be encouraged. The businesses and trade groups that comprise this group of commenters, however, believe that requiring companies to undertake and publicize their PIAs would institute an unnecessary expense on many businesses and, in many cases, may contribute to misinformation due to consumer confusion over the substance of the PIAs. Furthermore, required disclosure would undermine one of the fundamental benefits of the PIA – open and thorough analysis. Commenters claim that forced publication would severely affect the likelihood that companies would engage in full and deep analysis of their business practices. Many firms are concerned that innovation would suffer because companies would be reluctant to discuss new ideas knowing that PIAs would be published and seen by their competitors.

FTC or DoC

If new legislation is enacted, it is uncertain which agency will spearhead its implementation. Businesses with multinational ties, and the trade groups that represent them, generally prefer that the DoC either direct this effort or, at the very least, play a prominent role. They note that the DoC has the expertise, position and ability to develop the baseline framework, educate consumers and industry and provide guidance and a forum for the development of technological standards and industry codes. Equally important is the fact that the DoC can represent business interests abroad, thereby ensuring that cross-border data transfer rules protect consumers without unnecessarily impeding the free flow of information, creating barriers to international trade or hurting the competitiveness of U.S. businesses.

Consumer groups, conversely, are not as confident that the DoC will support the interests of individuals. Many of them fear that the DoC will seek only to serve the interests of businesses and neglect the question of consumer rights. Instead, they prefer that the FTC be empowered to direct enforcement. If this happens, a number of these groups favor limiting the FTC's authority; specifically, they want to require the FTC to partner with non-governmental organizations in its enforcement efforts. They also suggest that other governmental groups—state attorneys general for one—remain empowered to enforce the legislation under their current control.

Conclusion

As we mentioned in the last issue, while neither agency has announced when they will issue final versions of their reports, they are expected later this year. Additionally, congressional activity on privacy issues may affect some of the proposals put forth by the FTC and DoC: As mentioned above, Congresswoman Jackie Speier recently introduced DNT legislation; Senator John Kerry is considering comprehensive privacy legislation, and, shortly before this article was published, the Senate

Commerce Committee held a hearing on privacy issues, at which representatives from both the FTC and DoC testified. From any angle, 2011 promises to be a major year for privacy policy in the U.S.

This article first appeared on April 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.*