Hogan Lovells

December 2010

Privacy and Information Management Alert

FTC privacy report and Department of Commerce green paper raise important questions on commercial use of information about people

Commission staff outlines privacy protections businesses will be expected to provide as collection technologies advance

Commerce staff proposes new laws and new federal privacy office

What businesses should be doing as reports are finalized

Introduction

December 2010 will go down as the month when the U.S. federal government gave more attention than ever to issues of consumer privacy. Both the Federal Trade Commission (FTC), the nation's chief consumer protection agency, and the Department of Commerce issued reports proposing significant changes in the way businesses handle consumer information and changes in the control consumers would have over their information. We address each in turn.

The Federal Trade Commission preliminary staff report

- Should privacy law protections extend to information about consumers collected offline as well as online?
- For purposes of privacy protection, is it time to dispense with the distinction between personally identifiable information (PII) and non-PII in an age when technology can piece together data fragments to reveal personal details about consumers?
- Should businesses provide clearer and more relevant notice and choice, and follow the additional Fair Information Practice Principles (FIPPs) of collection limits, use of data only for the intended purposes of collection, and personal access to collected information? Are there certain uses of information that are so commonly understood that notice is less important?
- Is "Privacy By Design" a concept that all businesses handling information about people should follow?
- Should consumers be afforded an opportunity to avoid online tracking through a "Do Not Track" mechanism?

The preliminary FTC staff report issued on 1 December 2010 entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (the Report) answered each of these questions with a resounding "Yes."

But what does it mean for businesses that collect and use information about consumers? Must they change their practices immediately? Does the Report signal a new enforcement paradigm for the FTC under Section 5? Is it a call for legislation?

In the Report and in public comments about the Report, FTC officials have made it clear that the existing privacy framework, developed by over forty years of FTC guidance and enforcement, remains in place, but that improvements are necessary given technological advances in the collection, use, sharing, and retention of information about consumers by businesses. The Report signals the direction that the FTC Staff believes privacy protections should move, and the Commissioners themselves endorsed the concepts by voting unanimously to release the Report.

But given the absence of rulemaking authority for the Commission under Section 5 of the FTC Act, and the requirement that consumers must suffer a traditional type of harm prior to the FTC invoking its enforcement authority, the Report does not constitute a new set of rules or express enforcement warnings. To the contrary, the only express call for legislation in the Report is in the

context of its call for the implementation of a Do Not Track mechanism, but even that is proposed in the alternative, with self-regulation cited as an alternative mechanism for achieving Do Not Track protections. Notably, the Report criticizes the slow progress made by self-regulation in certain respects, but it remains that with limited FTC authority in the area of privacy and data security, self-regulation will be relied upon for some time to come.

The Report is expressly labeled "preliminary" in order to continue the discussion started more than a year ago with the FTC's three-part privacy roundtables. Moreover, many of the concepts articulated are at a high level, prompting the FTC Staff to pose a series of questions for which input is requested.

Appended to the FTC's Report are sixty-four questions on which interested parties are invited to comment, and these questions are attached to this Special Report. Based on these comments, which the FTC has requested by 31 January 2011, the Commission intends to issue a final report later in 2011.

Development of the proposed framework

The Report outlines the FTC's current approach to privacy protection, discusses the feedback it has received regarding the limitations of that approach, and then details the specifics of its new proposed framework.

The FTC's current approach to privacy protection: the "notice-and-choice" and "harm-based" models

The Report first described the two major frameworks under which it historically evaluated consumer privacy: the notice-and-choice and harm-based models. The notice-and-choice model represents the FTC's use of its authority under Section 5 of the FTC Act,[1] which prohibits businesses from engaging in "unfair" or "deceptive" trade practices, to bring enforcement actions against companies that include deceptive statements in their privacy notices about their collection and use of consumer data. Under the harm-based model, the FTC has focused its privacy enforcement on the data use practices of commercial entities that caused or were likely to cause physical harm (such as risks to physical security from stalking), economic harm (such as economic injury resulting from identity theft), or invasive intrusions into consumers' daily lives (such as from the receipt of unwanted solicitations).

Addressing limitations of the FTC's current approach

In recent years, critics of the notice-and-choice and harm-based models have alleged that they have not been sufficient to protect consumer privacy in the U.S. In response to these criticisms, the FTC held a series of three public roundtable discussions from December 2009 to March 2010 for interested stakeholders to explore the effectiveness of its current approach to privacy.[2] The FTC drew five major conclusions from these discussions:

- The collection and use of consumer data has increased. Some participants noted that data collection has become ubiquitous, pointing to the rapid growth in data processing and storage capabilities, advances in online profiling, and the aggregation of information from online and offline sources;

- A lack of understanding undermines consumers' ability to make informed choices about the collection and use of their data. Some participants discussed that privacy policies are difficult to locate and understand and that consumers do not understand the extent to which their data is shared with third parties;

- Consumers actually care about their privacy. Some participants pointed to consumer surveys showing discomfort with online tracking and consumer interest in using new privacy-enhancing technologies;

- Benefits flow to consumers from data collection and use. Some participants urged the FTC to adopt a flexible approach in order to allow for industry innovation and to support the wealth of free Internet content and functionality that is supported by online advertising;

[1] 15 U.S.C. § 45.

[2] *See FTC, Exploring Privacy – A Roundtable Series* (Dec. 7, 2009), http://ftc.gov/bcp/workshops/privacyroundtables/index.shtml. The second and third roundtable events took place on January 28, 2010, and March 17, 2010.

- The distinction between PII and non-PII is diminishing. Some participants noted the existence of technologies that permit companies to combine pieces of purportedly anonymous data and "re-identify" that data to a specific consumer, and how this militates in favor of eliminating the legal distinction between PII and "anonymized" data.

Given these conclusions, the FTC outlined in the Report what it perceived as being the major issues with its existing privacy regime. Regarding the notice-and-choice model, the FTC commented that notices to consumers about privacy practices often are buried in long, difficult-to-understand privacy policies. It stated that consumers frequently lack true choices about how their data is used, either because companies fail to give consumers specific avenues to choose or because the ability to choose is not readily apparent. Additionally, the FTC acknowledged that the harm-based model fails to recognize certain intangible consumer harms such as reputational harm and the fear of being monitored. Finally, though it acknowledged that current industry attempts to address these problems through self-regulation are steps in the right direction, the FTC urged increased self-regulation as a viable way to address the problems outlined in the Report.

The proposed framework

The FTC did not suggest that the notice-and-choice and harm-based models should be discarded altogether. Instead, it proposed using them as the foundation for a more robust framework for the protection of consumer data collected and used by commercial entities.

The framework, which the FTC stated should apply to all businesses that collect, maintain, share, or otherwise use consumer data either online or offline, contains three top-level maxims:

- Privacy by design. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services. This includes incorporating substantive privacy protections – such as data security and retention practices – into business processes and maintaining comprehensive data management procedures throughout the lifecycle of products and services;

- Simplifying consumer choice. Companies should simplify consumer choice, not just through notice about privacy practices prior to the use of a product or service in a lengthy privacy policy, but by offering choice at a time and in a context in which the consumer is making a decision about his or her data (such as when the consumer is presented with a targeted online behavioral advertisement);

- Increasing consumer transparency. Companies should increase the transparency of their data practices, such as by clarifying, shortening, and standardizing privacy notices; providing reasonable access to the consumer data they maintain; providing prominent disclosures and obtaining affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected; and working to educate consumers about commercial data privacy practices.

One specific proposal contained within the Report under the theme of simplifying consumer choice is a "Do Not Track" mechanism that the FTC contemplates could be advanced either by legislation or enforceable industry self-regulation. Such a mechanism would require businesses to comply with a consumer's centralized opt-out of online behavioral tracking. Notably, the Report provided no specifics regarding what such legislation or self-regulation might look like, though in subsequent comments, FTC representatives have stated that the Commission would prefer Do Not Track to be enforced through self-regulation.

The most significant feature of the framework may be what it was not: a set of prescriptive rules that create discrete, enforceable compliance obligations. Instead, the Report urges industry to adopt certain best practices embodied in the framework, and it seems clear that the framework will color FTC enforcement in the future.

Analysis of the proposed framework and implications for business

Though the FTC does not have the authority to adopt the framework into formal, enforceable regulations, to the extent that any of the framework's principles touch on themes from past Section 5 enforcement actions, the Commission likely will try to incorporate these principles into future privacy enforcement. The principles that carry the highest risk for companies are those that are more

closely tied to recommendations in existing enforcement actions, such as the recent *Sears* and *EchoMetrix* enforcement actions for deceptive privacy notices (discussed later in this Special Report).

Given the scrutiny that the FTC will likely apply to privacy practices following the issuance of the Report, companies that collect, maintain, use, or share personal information should undergo an assessment of their data practices for compliance with existing privacy law and precedent if they have not done so recently. In addition to areas of historical FTC enforcement, companies should review their privacy practices generally to see how they stack up to the Commission's desired level of privacy protection under its new framework. If past enforcement is any indication, the FTC's next target likely will be among the "low-hanging fruit" of privacy violations; that is, an egregious, high-profile privacy breach that could have been prevented by following the framework.

While deterrence from enforcement certainly will be a primary motivation for some companies to reevaluate their data practices, the framework reflects some privacy best practices that not only will help ensure compliance with the law but also will help create a better marketplace for consumers, and perhaps create a competitive advantage for companies.

The concepts advanced by the Report

Commonly accepted data uses and offering consumer choice

One of the new concepts introduced in the Report is that companies do not necessarily need to receive consumer consent before using that consumer's data for certain "commonly accepted" purposes. Receiving consent for such practices would be unnecessary because the data use is obvious or necessary for public policy purposes. For example, a consumer who orders a product online should not have to consent to the use of that address in the delivery of the purchased product. Under such a rule, companies would be able to eliminate these uses from their privacy notices, and consumers would benefit from being able to focus their attention on privacy practices that are more likely to be controversial.

Based on the information it gathered in its roundtable discussions, the FTC preliminarily indicated that it will consider the following categories of practices as commonly accepted practices:

- Product and service fulfillment, such as the use of addresses for shipping, credit card information for payment, and data entered into an online application for use within that application;
- Internal operations, such as customer satisfaction surveys and website analytics;
- Fraud prevention, such as the use of identity-verification technologies, the review of server logs, and use by brick-and-mortar stores of undercover employees and video cameras to monitor against theft;
- Legal compliance and public purpose, such as subpoena compliance and credit reporting; and
- First-party marketing, such as the recommendation of products or the delivery of coupons based upon prior purchases.

This recognition that privacy requirements be relaxed in these circumstances evinces a greater concern by the FTC for industries that make secondary use of data obtained from other sources. The industries likely most affected by this approach would include data brokers, operators of online targeted advertising networks, and any other businesses that profit from the use of consumer data without a direct relationship with the consumer. Notably, the FTC commented that third-party service providers could also take advantage of the commonly accepted carve-outs, so long as they only use the consumer data received in the performance of the commonly accepted purpose.

In its requests for comment, the FTC posed a number of questions about what should constitute a commonly accepted practice. Among other questions, it asked whether companies should be able to rely on the exception for first-party marketing when the information collected qualifies as sensitive data, such as medical data. Additionally, it asked whether a company should be allowed to rely on this exception to send advertisements to consumers through different media than through which information was collected, such as by sending a text message advertisement based on a consumer's online search query. It also asked whether the proposed first-party marketing rule should extend to commonly branded affiliates, and the nature of the choice that should be provided to

consumers regarding the practice of data "enhancement" by which companies enrich customer databases with data from other sources.

Do Not Track mechanism

Currently, the primary methods by which consumers can opt out of online behavioral tracking are by regularly deleting tracking cookies, by utilizing tools that prevent all cookies from being stored on their browsers (such as a "private" browsing mode), or by downloading broad "opt-out" cookies that notify participating advertisers that the user does not wish to be tracked. All of these methods, the FTC recognized, have flaws. Regularly deleting cookies is cumbersome on consumers, and it is sometimes hard to distinguish between tracking cookies and other cookies a consumer may wish to retain, such as session cookies. Tools preventing the storage of all cookies have a similar effect, prohibiting consumers from the benefits of non-tracking cookies they wish to retain. Opt-out cookies may not be updated frequently enough, are of limited duration, and risk being deleted along with consumers' other cookies. The goal of the development of a Do Not Track mechanism would be to ensure, industry-wide, that consumers are never tracked online when they do not wish to be.

The Do Not Track proposal has garnered a lot of attention since the release of the Report because it is one of the few specific examples of how the FTC prefers industry to meet the framework's objectives. Since the release, however, FTC Director of the Bureau of Consumer Protection David Vladeck has dispelled various rumors about Do Not Track. Despite the Report's mention of a browser plug-in as a possible method of effectuating Do Not Track, Vladeck has emphasized that the Commission does not wish to delineate a specific technology for industry to use. This indeed may be the wisest approach, as given the freedom and flexibility to develop the most relevant technologies, industry should be able to create the best market-tested solution to prevent unwanted tracking without having to be pigeonholed into a particular technology. Also, despite both self-regulation and legislation being mentioned in the Report as possibilities to implement Do Not Track, Vladeck has stated the FTC's preference for the development of a self-regulatory solution.

Taking this cue, industry has already started exploring Do Not Track solutions. For example, Microsoft recently publicized plans to build such functionality into the upcoming release of its Internet Explorer browser.[3] And despite the FTC's preference for a self-regulatory solution, Congress held hearings on possible Do Not Track legislation the day after the release of the Report.[4]

The Report asks for comments on a number of issues pertaining to Do Not Track, such as how a universal mechanism can be best designed to be clear and understandable for consumers; the potential costs and benefits of offering a standardized uniform choice mechanism for online behavioral advertising; historical utilization of opt-out mechanisms; the impact if a large number of consumers opt out; whether consumers should be presented with more granular options on the types of advertisements to receive; and whether a Do Not Track mechanism should be required for different media, such as mobile devices.

Narrowing the distinction between PII and non-PII

One of the major themes that emerged from the roundtable discussions held by the FTC was how increases in technology and computing power are blurring the line between what constitutes PII and what does not. The Report noted that for advertising purposes, the more information a company can accumulate about a consumer, the more valuable that information becomes. This truism, according to the FTC, has created an incentive to "re-identify" the subjects of even supposedly anonymous data elements to maximize the ability to market those elements to advertisers. As examples, the Report pointed to recent situations in which companies have released purportedly "anonymized" data sets only to find that researchers were able to associate the released data with specific individuals.

The FTC incorporated these concerns into its proposed framework by applying protections to all consumer data that "can be reasonably linked to a specific consumer, computer, or other device." In doing so, it would abandon its typical requirement that for there to be a privacy violation, data needs to be tied to an identified individual. According to this reasoning, companies would no

[3] Peter Cullen, Chief Privacy Strategist, Microsoft, *Online Privacy & Balance – Our Perspective* (Dec. 7, 2010), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/12/07/online-privacy-amp-balance-our-perspective.aspx.

[4] Hearing of the House Subcommittee on Commerce, Trade, and Consumer Protection, "Do Not Track Legislation: Is Now the Right Time?" (Dec. 2, 2010), *available at* http://energycommerce.house.gov/index.php?option=com_content&view=article&id=2147.

longer be able to rely on the argument that there can be no privacy violation if the only data elements they maintain are anonymous, if those data elements are tied to a unique identifier. This idea has also appeared in recent legislative proposals before Congress that would require privacy protections to be applied whenever data can be associated with a unique identifier,[5] so this is one of the themes from the Report that we believe is most likely to gain legislative traction in the future.

In its requests for comment, the FTC asked whether it is possible to conclusively define when data should be considered "linkable" to a specific consumer, computer, or other device, given that the more data elements that are combined, the greater probability that those elements may be used to identify an individual. It has also asked whether technical measures exist to effectively anonymize data and whether any industry norms are emerging in this area.

Standardization of privacy notices

One of the Report's major criticisms was that privacy notices are often very difficult for consumers to understand. The FTC pointed out that many privacy policies are "opaque, lack uniformity, and are too long and difficult to navigate." In addition, newer technologies may pose additional problems such as the limited space on mobile devices on which to display privacy notices.

To address this issue, the Report stated that privacy notices should be standardized on two levels. First, a business should standardize its policies internally, using similar formats and terminology across all of its privacy policies. Second, privacy policies should be standardized across companies, as is the case with the layered privacy notices required for financial institutions under the Gramm-Leach Bliley Act. The Report seeks comment on the feasibility of creating standardized notices and how notices should be tailored in light of rapidly advancing technology.

While it is unclear whether the FTC will eventually endorse a standardized privacy notice, the FTC has already brought enforcement actions against privacy notices that it views as being insufficient, making this an area ripe for future enforcement based on the framework. For example, the FTC's recent *Sears* and *EchoMetrix* enforcement actions (the latter of which was publicized the day before the release of the Report) have indicated the agency's willingness to bring deception claims against companies that bury important privacy disclosures deep within long privacy policies.[6] These actions dovetail with the Report's focus on increasing the transparency and simplicity of privacy policies, and give the FTC a hook through which it is more likely to enforce that aspect of the privacy framework in the future.

Based on the Report and these recent settlements, companies should make sure that their privacy practices are clearly described and not buried in their privacy notices, highlighting data practices that consumers are likely to find material. Additionally, companies might consider adopting layered privacy policies through which consumers can initially view a concise summary of privacy practices and click through to more specific details if so desired.

Delivery of "just-in-time" privacy disclosures and the FTC's view of self-regulation

In addition to increasing transparency of privacy notices, the FTC also indicated that privacy disclosures would be more effective if delivered at the point in time at which a consumer provides data, rather than relying on consumers to review and remember a privacy policy prior to using a website. The FTC further suggested that for social media services, disclosures should be made when

---

[5] *See, e.g.,* Hogan Lovells Chronicle of Data Protection, *Rep. Rush Introduces Privacy Bill to Regulate Collection and Use of Personal Information*, http://hldataprotection.com/2010/07/articles/legislation/rep-rush-introduces-privacy-bill-to-regulate-collection-and-use-of-personal-information (July 21, 2010) (describing § 2(4)(A)(vii) of H.R. 5777, introduced this past July, that covers within its scope data tied to "any unique persistent identifier . . . where such identifier is used to collect, store or identify information about a specific individual or to create or maintain a preference profile").

[6] In *Sears*, the FTC obtained a consent decree from a company that informed consumers participating in a promotion that it would download tracking software onto their computers, but buried the details of the tracking in a notice deep within a lengthy terms of service agreement that showed up only at the end of a protracted registration process. *Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (2009), *available at* http://ftc.gov/opa/2009/06/sears.shtm. Building on the *Sears* enforcement, the FTC in *EchoMetrix* obtained a consent decree where the company informed users of parental monitoring software that it could use data collected "to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients," but did so in the thirtieth paragraph of a policy that was contained in a small scroll box that was presented to users when registering for the service. *EchoMetrix, Inc.*, FTC File No. 102-3006 (Nov. 30, 2010), *available at* http://ftc.gov/opa/2010/11/echometrix.shtm. The FTC objected when the company used this disclosure to justify the incorporation the data of children of parents who used the software, including website history and instant messages, into a product that provided third parties with aggregate consumer opinions.

a consumer decides to use an application that collects data or, if information sharing occurs automatically, disclosure should be made at the time a consumer becomes a member of the social media service.

This position is not new. For example, the FTC has consistently advocated for a "just-in-time" approach for notice to consumers in the online behavioral advertising context.[7] Over the past few years, industry has taken concrete steps toward implementing this approach. This past July, a number of major advertising industry groups announced that they would be incorporating the "Power I," an icon developed by the Future of Privacy Forum that alerts consumers to the existence of a targeted advertisement,[8] into their self-regulatory programs.[9] The FTC's support for self-regulation is also apparent in its stated desire to implement a Do Not Track mechanism through self-regulation rather than legislation.

The real issue the FTC has had regarding self-regulatory efforts is their rate of adoption. So long as industry adoption of positive self-regulatory practices is not widespread, some consumers will go unprotected and the FTC will grow increasingly impatient. Nevertheless, the FTC has not given up on self-regulation, though it certainly will be looking for even more activity from industry in the near future.

Companies should heed the Report's call and work expediently to more widely implement self-regulatory practices, such as just-in-time privacy notice, that are both beneficial to consumers and being flexible in their implementation. With no explicit prescriptions in the Report, companies have an excellent opportunity to creatively develop privacy-enhancing technologies and business practices to address some of the issues raised by the FTC. Companies also can work to make their own privacy practices more transparent and efficient, and industry groups and coalitions can work to standardize practices and encourage widespread adoption. The ability to advance these self-regulatory efforts will play a major role in shaping the FTC's privacy framework, enforcement strategy, and legislative recommendations.

Material changes to privacy practices

While it is well-settled FTC precedent that a company must prominently provide notice and receive consumer opt-in consent if the company materially changes the way it will treat PII already collected, the exact contours of what constitutes such a "material change" are fuzzy. To that end, in the Report the FTC requested comment on exactly what should constitute a "material change." Companies that frequently change or are considering changing their privacy practices or notices in the future may wish to comment on this issue, as a broader definition of what constitutes a material change could greatly impede the ability to make such changes without having to wait and account for individualized opt-in consent.

Closing the gap between U.S. and EU data protection

On 11 November, the European Commission (EC) released a report recommending reforms to the EU's approach to privacy entitled "A comprehensive approach on personal data protection in the European Union" (the Draft Agenda).[10] Both the FTC Report and the EC Draft Agenda have the goal of discussing the regulators' desired approach to data protection, and some of the specific proposals draw on similar themes. In the Draft Agenda, the EC outlined a number of issues it hopes to address as it works to revise the EU Data Protection Directive. Much like the FTC Report, the EC Draft Agenda is the first step in a process that may ultimately end with changes to the privacy legal regime.

---

[7] In its 2009 report on online behavioral advertising, the Commission commended businesses that that placed disclosures in close proximity to advertisements with links to the pertinent section of a privacy policy explaining how data is collected for the purposes of delivering targeted advertising. See FTC STAFF, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 35-36 (2009), available at http://ftc.gov/os/2009/02/P0085400behavadreport.pdf

[8] *See* Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, *available at* http://nytimes.com/2010/01/27/business/media/27adco.html.

[9] Am. Ass'n of Adver. Agencies, Ass'n of Nat'l Advertisers, Direct Mktg. Ass'n, Interactive Adver. Bureau, & Council for the Better Bus. Bureaus, Trade Groups Announce the Selection of the Wording and Link/Icon that Will be Used to Indicate Adherence to Industry Self-Regulatory Principles for Online Behavioral Advertising (Jan. 27, 2010), *available at* http://the-dma.org/cgi/dispannouncements?article=1379.

[10] EUROPEAN COMM'N, COMMUNIC'N FROM THE COMM'N TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECON. & SOCIAL COMM. & THE COMM. OF THE REGIONS: A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION, COM(2010) 609 (Nov. 4, 2010) *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

Though the U.S. and EU currently have different baseline privacy protections, there are some substantive similarities between the reports, and some instances in which the FTC encourages the adoption of more European-style protections. For one, the FTC Report expressed an interest in Privacy by Design, a framework developed by the Privacy Commissioner of Ontario, Dr. Ann Cavoukian, that provides a set of guiding principles encouraging information system owners to proactively and pervasively incorporate privacy protections into the design of their systems.[11] On the European side, the EC's Draft Agenda also suggests the possibility of a concrete implementation of the Privacy by Design concept. In another example, the FTC lists substantive privacy protections that should be included as part of an organization's privacy infrastructure such as data security standards, limits on data collection, data retention policies, and data accuracy policies. These privacy protections are similar to provisions already found in the EU Data Protection Directive. The FTC's framework also stresses the importance of implementing comprehensive data management procedures, such as conducting regular privacy training and assessments, while the EC Draft Agenda suggests the mandating the appointment of a Data Protection Officer for companies of a certain size and requiring data controllers to perform a "data protection impact assessment" in certain situations. In addition, both proposals discuss ways to increase the transparency and standardization of privacy notices.

The difference in baseline privacy protections between the jurisdictions, however, still produces some significant gaps in the respective reports' aspirational approaches to privacy. For example, in taking a step closer to one of the tenets of EU privacy law, the FTC stated in its Report that businesses should provide consumers with "reasonable access" to data that the company maintains about them. The FTC Report, however, qualifies that the right to access should operate on a sliding scale, proportional to the sensitivity of the data and the costs to the company. A more stringent right to access currently exists in the EU legal framework, and the EC Draft Agenda even seeks to strengthen this right by including proposals for a "right to be forgotten," for requiring a right to data portability, and for improving the functioning of current access mechanisms.

While the European approach to privacy is currently much more detailed and prescriptive, the FTC Report contains concepts that are currently present under the EU Data Protection Directive and has significant parallels to the EC's Draft Agenda. This observation is shared by European Data Protection Supervisor Peter Hustinx, who expressed this opinion in a meeting with members of the Hogan Lovells global Privacy and Information Management Practice shortly after the release of the FTC Report.[12] In this meeting, Mr. Hustinx also suggested that the FTC Report may help pave the road for the day when the U.S. privacy framework will be recognized by the EU as providing "adequate" protection, allowing for the free cross-border transfers of data between the EU and U.S. While he suggested that this likely would not occur in the immediate future, he commended U.S. efforts aimed at advancing consumer privacy protections through the issuance of the FTC Report.

Concurring opinions

Though voting to issue the Report, Commissioners Kovacic and Rosch filed concurring statements. Both Commissioners indicated that while they were interested in seeing public comments on the Report, they each had reservations about certain aspects of the proposed framework. Commissioner Kovacic suggested that the introduction of a Do Not Track mechanism is premature, and that before proceeding the FTC should provide more background on how the current framework builds on earlier FTC enforcement approaches and more evidence on how consumer expectations have been unmet. The Commissioner posed a number of his own questions for public comment pertaining to these points.

Though concurring in its issuance, Commissioner Rosch suggested that the proposed framework is unnecessary to protect consumer privacy. Rather, he suggested that the FTC more actively enforce its existing privacy approach by continuing to bring enforcement actions when consumers are not provided with proper notice. Rosch also objected to the implication in the Report that a theoretical and untested choice-based approach should replace the existing notice-based model.

While both Kovacic and Rosch had concerns about aspects of the proposed FTC framework, both Commissioners ultimately voted to release the Report to receive public comments on the proposals and to continue the dialogue on these issues. Their views will likely be shared by many in industry, and the resulting dialogue should yield interesting discussions and comments leading to the publication of the final report. This tension might point to a philosophical disagreement within the Commission regarding how far it

[11] *See* Privacy by Design, http://privacybydesign.ca.

[12] *See* Hogan Lovells Chronicle of Data Protection, *EU Data Protection Supervisor's Interview at Hogan Lovells London* (Dec. 3, 2010), *available at* http://hldataprotection.com/2010/12/articles/international-compliance-inclu/eu-data-protection-supervisors-interview-at-hogan-lovells-london.

believes it can extend its enforcement power under Section 5 of the FTC Act. Part of the reservation on the part of Kovacic and Rosch may also point to the desire to refrain from any major changes until Congress has legislated these issues – either as a comprehensive online privacy bill or smaller, issue-based legislation such as Do Not Track – or has given the FTC some sort of rulemaking authority to regulate privacy above and beyond the authority currently extended by the FTC Act.

The Commerce Department green paper

U.S. policy on privacy has not just been an endeavor of the FTC. A little over two weeks after the release of the FTC report, the Department of Commerce released its green paper entitled "Privacy and Information Innovation: A Dynamic Privacy Framework for the Internet Age,"[13] which argued that preserving consumer privacy online and thereby bolstering consumer trust in the Internet is essential for businesses to succeed online.

The green paper was authored by the Internet Policy Task Force at Commerce – a joint effort of the Office of Commerce Secretary Gary Locke, the National Telecommunications and Information Administration, the International Trade Administration, and the National Institute of Standards and Technology. The paper follows a Notice of Inquiry to which many stakeholders responded, and a symposium last May.

The green paper says there is a "compelling need to provide additional guidance to businesses, to establish a baseline privacy framework to afford protection for consumers, and to clarify the U.S. approach to privacy to our trading partners – all without compromising the current framework's ability to accommodate new technologies."

Like the FTC Report, the Commerce green paper proposes an expanded set of FIPPs, yet it is stronger than the FTC Report in raising the prospect of baseline privacy legislation, and it directly raises the question of whether the FTC should be given rulemaking authority to implement privacy principles (which it now lacks under Section 5 of the FTC Act). The green paper also suggests a safe harbor provision in any legislation, for companies that adhere to "voluntary, enforceable codes of conduct."

The paper cautions that any new laws should not preempt the strong sectoral laws that already provide important protections, but rather should act in concert. The paper also recognizes the important role state law has played in building the privacy and data security framework in the U.S., and it cautions against impairing the states' role as privacy law incubators. In addition, the role state Attorneys General can play in enforcing privacy rights is expressly recognized in the green paper.

With respect to full implementation of the FIPPs, the paper specifically has in mind enhancing transparency, encouraging greater detail in purpose specifications and use limitations, and fostering the development of verifiable auditing and accountability programs. The idea of Privacy Impact Assessments also is discussed.

The green paper also calls for a federal data security breach notification law for electronic data.

The Commerce paper also calls to reforming the opaque and outmoded Electronic Communications Privacy Act (ECPA), paying particular attention to assuring strong privacy protection in cloud computing and location-based services. The goal of this effort is to ensure that, as technology and market conditions change, ECPA continues to provide a fair balance between individuals' expectations of privacy and the legitimate needs of law enforcement to gather the information it needs for security.

The absence of a designated privacy authority in the federal government also is addressed in the green paper, and there is a call for a Privacy Policy Office (PPO). The office would not have enforcement authority – the FTC would continue to play the lead privacy enforcement role.

In his 27 October speech at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem,[14] NTIA Administrator Lawrence E. Strickling explained that the PPO "would complement, not supplant, the Federal Trade Commission or

---

[13] U.S. DEP'T OF COMMERCE INTERNET POL'Y TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (Dec. 16, 2010), *available at* http://ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[14] Lawrence E. Strickling, Ass't Sec. of Commerce for Commc'ns & Info., U.S. Dep't of Commerce, Remarks on Privacy and Innovation (Oct. 27, 2010), *available at* http://ntia.doc.gov/presentations/2010/IntlConfDataProtectionPrivacyCommissioners_10272010.html.

the other institutions of the Federal Government, such as the professional cadre of Chief Privacy Officers we now have in multiple agencies. A key role for the new Privacy Office would be to bring together the many different parties that are necessary to help develop privacy practices."

Mutual international recognition of and respect for privacy frameworks also is mentioned in the green paper, a reference to the EU's persistent finding that the U.S. lacks "adequate protection" of personal data, thus requiring cumbersome legal mechanisms for the cross-border transfer of data. As mentioned above, further movement by the U.S. toward more European-style privacy protections can go a ways towards an adequacy finding in the EU and obviating the need for these legal mechanisms.

Like the FTC Report, the Department of Commerce requests comment on a number of questions contained within the green paper. These questions include whether there is a need for federal legislation in the area, and whether there should be a federal private right of action for privacy violations. It is expected to publish further questions in the Federal Register (to be released after the publication of this Special Report), and has requested comments from interested parties by 28 January 2011.

Conclusion

The publication of the FTC Preliminary Report and the Commerce green paper are significant moments for privacy in the United States. The documents provide a solid framework consisting of best practices that organizations wishing to be privacy leaders would benefit from adopting. In addition, failure to implement certain recommendations could spur further legislative action in the area, which in turn could hamper businesses in their efforts to develop flexible privacy-enhancing technologies and business practices to help ensure consumer privacy while still being able to use data in a way that ultimately provides benefits to consumers.

The FTC's final report and the green paper could be significantly influenced by comments to the sixty-four questions appended to the FTC Preliminary Report and the questions posed throughout the Commerce green paper, so interested parties should submit their comments prior to the 31 January FTC deadline and the 28 January Department of Commerce deadline.

For more information, please contact:

WASHINGTON, DC
Christopher Wolf
Partner
T +1 202 637 8834
christopher.wolf@hoganlovells.com

WASHINGTON, DC
Eric Bukstein
Associate
T +1 202 637 2749
eric.bukstein@hoganlovells.com

WASHINGTON, DC
Bret Cohen
Associate
T +1 202 637 8867
bret.cohen@hoganlovells.com

Hogan Lovells Chronicle of Data Protection
Subscribe to the complimentary source for privacy and information commentary at www.hldataprotection.com.

Questions for Comment on Proposed Framework

QUESTIONS FOR COMMENT ON PROPOSED FRAMEWORK

Scope

- Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

- Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?

- How should the framework apply to data that, while not currently considered "linkable," may become so in the future?

- If it is not feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device," what alternatives exist?

- Are there reliable methods for determining whether a particular data set is "linkable" or may become "linkable"?

- What technical measures exist to "anonymize" data and are any industry norms emerging in this area?

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

Incorporate substantive privacy protections

- Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

- Should the concept of "specific business purpose" or "need" be defined further and, if so, how?

- Is there a way to prescribe a reasonable retention period?

- Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?

- How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

- When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?

- Can companies minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests?

Maintain comprehensive data management procedures

- How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

- What roles should different industry participants – *e.g.*, browser vendors, website operators, advertising companies – play in addressing privacy concerns with more effective technologies for consumer control?

Companies should simplify consumer choice

Commonly accepted practices

- Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

- Are there practices that should be considered "commonly accepted" in some business contexts but not in others?

- What types of first-party marketing should be considered "commonly accepted practices"?

- Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?

- Should first-party marketing be limited to the context in which the data is collected from the consumer?

    - For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes first-party marketing. An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumer's prior purchases in the store. Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context – for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?

- Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?

- How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?

Practices that require meaningful choice

General

- What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?

- Should the method of consent be different for different contexts?

    - For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen?

    - Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?

    - Is there market research or are there academic studies focusing on the effectiveness of different choice mechanisms in different contexts that could assist FTC staff as it continues to explore this issue?

- Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

- What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?

    - In particular, how should companies communicate the "take it or leave it" nature of a transaction to consumers?

    - Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?

- How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?

- What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?

- What (if any) special issues does the collection or the use of information about teens raise?

    - Are teens sensitive users, warranting enhanced consent procedures?

    - Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach?

- What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?

- Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

Special choice for online behavioral advertising: Do Not Track

- How should a universal choice mechanism be designed for consumers to control online behavioral advertising?

- How can such a mechanism be offered to consumers and publicized?

- How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?

- How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?

- What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?

- How many consumers would likely choose to avoid receiving targeted advertising?

- How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?

- What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?

- In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that

allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?

- Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?

- If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

Companies should increase the transparency of their data practices

Improved privacy notices

- What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

- How can companies present these notices effectively in the offline world or on mobile and similar devices?

- Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

Reasonable access to consumer data

- Should companies be able to charge a reasonable cost for certain types of access?

- Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

- Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?

- Should access to data differ for consumer-facing and non-consumer-facing entities?

- For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?

- Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

- Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Material changes

- What types of changes do companies make to their policies and practices and what types of changes do they regard as material?

- What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

Consumer education

- How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

- What role should government and industry associations have in educating businesses?