ReedSmith

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this *Alert*, please contact one of the authors:

Paul Bond
Partner, Princeton
+1 609 520 6393
pbond@reedsmith.com

Chris G. Cwalina
Counsel, Washington D.C.
+1 202 414 9225
ccwalina@reedsmith.com

Amy S. Mushahwar
Associate, Washington, D.C.
+1 202 414 9295
amushahwar@reedsmith.com

Christine Nielsen
Associate,Chicago
+1 312 207 6459
cnielsen@reedsmith.com

Nick Tyler
Associate, London
+44 (0)20 3116 3695
ntyler@reedsmith.com

Fredrick Lah
Associate, Priceton
+1 609 524 2063
flah@reedsmith.com

...or the Reed Smith lawyer with whom you regularly work.

FTC Issues Final Commission Report on Consumer Privacy

Agency Calls on Companies to Develop Privacy Best Practices

Last week, the Federal Trade Commission (FTC) released its long-awaited final Commission Consumer Privacy Report entitled, "Protecting Consumer Privacy in an Era of Rapid Change" (Final Report). The FTC emphasizes that the Final Report only sets forth industry best practices and is "not intended" to serve as a new template for enforcement. However, this line is not exactly clear as the FTC identifies existing enforcement actions that form the basis of its advice (and could be the basis for section 5 enforcement actions).

The Final Report expands on a preliminary FTC staff report issued in December 2010 and is consistent with the Department of Commerce's (DOC) parallel privacy initiative. The Final Report calls on companies to do the following:

- **Engage in Privacy by Design**
- **Provide Simplified Choice**
- **Exhibit Greater Transparency**

Each of these initiatives will be described in further detail below.

The FTC calls on Congress to develop baseline privacy legislation with civil enforcement penalties to deter unlawful conduct. To this end, FTC Chairman John Leibowitz and DOC Assistant Secretary Lawrence Strickling testified last week before the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade to advance the legislative agenda. The hearing notice, archived hearing video, and Committee background memo are available here.

The Final Report also urges individual companies and self-regulatory bodies to accelerate the adoption of the principles contained in the Final Report, if they have not already done so. The FTC will work in the coming year to encourage privacy protections in five main areas, which were highlighted in the Final Report:

- **"Do Not Track" Browser Standard:** While the FTC commends the progress made by the Digital Advertising Alliance (DAA) in developing an icon-based system for self-regulation of the online advertising industry, it says that more work needs to be done. The DAA, Internet browser companies, the FTC and the DOC have publicly committed to implementing the existing DAA self-regulatory standard in a browser-based automated privacy tool that will help consumers persistently opt out of online behavioral advertising and multi-site advertising.
- **Mobile Data:** On the heels of the FTC Mobile Children's Privacy Report, the FTC continues to urge all companies offering mobile services to improve privacy disclosures. In that vein, the FTC will host a web-disclosure workshop including some mobile privacy discussions May 30, 2012, to address how mobile privacy disclosures may be streamlined for mobile screen viewing.
- **Data Brokers Disclosure & Consumer Data Access:** The FTC asks data brokers (those collecting information on consumers where they do not have a consumer-facing relationship) to create a centralized website where they would: (1) identify themselves to consumers and describe how they collect and use consumer data, and (2) detail the access rights and data choice they provide with the data that they maintain.
- **Large Platform Providers:** The FTC suggested that large platform providers, businesses such as ISPs, operating systems, browsers and social media companies that seek to comprehensively track consumers' online activities, raise elevated privacy concerns. This heightened concern regarding multi-platform tracking is best exhibited in the FTC's and state regulators' concerns regarding the streamlined Google privacy policy. FTC staff intends to host a public workshop on this topic in Q3 of this year.

- **Commerce's Development of Enforceable Self Regulatory Codes**: The DOC is in the process of developing sector-specific codes of conduct. FTC staff has indicated that it will participate in this process, and if strong privacy codes are developed in the Commerce process, the Commission will view adherence to such codes favorably when it is reviewing company practices under a section 5 action.

Below, we provide a detailed breakdown of the Final Report:

Scope of Harm

The FTC notes at the outset that the range of privacy-related harms implicated in this framework is more expansive than physical harm, economic harm or unwarranted intrusions. Per the FTC, any privacy framework should recognize the harms that might arise from "unanticipated uses" of data. The report suggests that harms could include the unanticipated sharing of private information and reputational harm, regardless of whether the data at issue is considered "sensitive" data.

Framework Application

The framework applies to all businesses that collect or use consumer data that can be "reasonably linked to a specific consumer, computer, or other device, unless the entity meets the small business exemption, it collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties." Notably, the framework also applies to offline or paper data. Data that has been permanently de-identified is exempt. From this standard, the FTC sheds further light on the following items:

- **Near Universal Compliance Expected:** All companies should comply with the framework, unless they meet the small business exemption.
- **Framework Works in Tandem with Existing Sector-Specific Law:** If any portion of the FTC's framework conflicts with existing sector-specific law, existing sector-specific laws govern.
- **"Reasonably Linkable" Standard:** Citing concerns voiced on the agency's comment docket regarding re-identification of anonymous data, the FTC chooses to identify a standard that was more expansive than traditional PII. But, we do not have a definition in the Final Report of what "reasonably linkable to a consumer, computer or other devise" means.
- **De-identified Data:** However, if data is de-identified, it is not "reasonably linkable" and doesn't raise privacy concerns. The Final Report clarifies that data is "not 'reasonably linkable' if a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." In a separate blog article, Ed Felten, FTC Chief Technologist, recognized that it is difficult to determine whether or not a data set is de-identified. However, he suggested as "a good rule of thumb: if you plan to use a dataset to personalize or target content to individual consumers, it's probably not de-identified."

Privacy by Design

Recognizing that many companies already employ Privacy by Design principles, the FTC outlines that companies should implement the following safeguards at every stage of the development of data products and services:

- **Data Security:** Companies should provide adequate data security. The FTC recognized the strong efforts of many industry players but still called for federal national breach standard legislation in this section that would authorize it to seek civil enforcement penalties.
- **Data Collection Limitations:** Companies should limit data collection to that which is consistent with the context of a particular transaction or the customer's relationship with the business, or as required by law. For any data collection outside of these contexts, the FTC recommends prominent concurrent disclosure – outside of the privacy policy.
- **Data Retention Practices:** Companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected. The FTC calls on trade associations to be more proactive in providing guidance to their members about data retention and destruction policies.
- **Data Accuracy:** Companies should improve on consumer data accuracy in accordance with the "intended use and sensitivity of the information." Companies using data to make decisions regarding a consumer's eligibility for credit and other important benefits should take "robust measures" to ensure data accuracy.

The FTC recommends that such protections be adopted pursuant to an organization-wide data privacy and security program. The FTC recognizes that such a program cannot be adopted overnight, and that issues such as legacy systems must be corrected or phased out over time.

Simplified Consumer Choice

The FTC retains the notice and choice model, and requests companies to provide a choice mechanism "at a time and context that is relevant to consumers – generally at the point the company collects the consumer's information." The FTC also recognized that choice is not necessary "for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law."

- **Examples of Practices That Do Not Require Choice:** The FTC proposes a list of commonly accepted practices – product and service fulfillment; internal operations; fraud prevention; legal compliance, public purpose; and first-party marketing (in many forms) – in which a company could engage without obtaining prior consumer consent. The Final Report, mindful of the concerns about such a static list, shifts the focus to the context of the transaction. The commonly accepted practices are maintained as illustrative examples of practices that may be consistent with the context of the transaction or the company's relationship with the consumer. This focus on context brings the FTC Report in closer harmony with DOC's report.
- **First-Party Marketing & Choice:** With respect to first-party marketing, the Final Report makes clear that a choice mechanism may be required if the practice is inconsistent with the context of the consumer's first-party interaction. For example, the flavor of online behavioral advertising known as "retargeting," in which the consumer is delivered an ad based on his or her previous activity on a retailer's website, is arguably first-party marketing. But, the Commission made clear that because the first-party marketer is now tracking the consumer on a third-party website, consent is now necessary.
- **Affiliates:** Affiliates are third parties, and a consumer choice mechanism is necessary unless the relationship is clear to consumers.
- **Choice & Data Enhancement:** The Final Report also tackles the issue of choice for data enhancement, which is the practice of appending additional data from third-party sources to data already gathered directly from the consumer. Even though the FTC considers transfer of data from one business to another to be inconsistent with the relationship the consumer has with the first-party business, the FTC stops short of recommending a choice mechanism in this context. The FTC recognizes the practical and logistical hurdles to providing choice, and states that compliance with other principles in the framework will adequately address concerns about data enhancement.

However, the FTC identifies that for practices inconsistent with the context of their interaction with consumers, companies should give consumers choices. For those practices requiring choice, the FTC provides some guidance stating "companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."

- **Choice Timing:** The FTC proposes a choice mechanism that was at a time and in a context

in which the consumer is making a decision about his or her data. Just-in-time notices may be different across different industries and practices within a particular industry. This principle offers some flexibility by recognizing that the time a consumer is making a choice about his or her data differs with the type of transaction.

- **"Take It or Leave It" Choices:** These should be disclosed prominently and, per the FTC, may be inappropriate for important services where consumers have few options in the marketplace for a particular good or service.
- **Do Not Track Mechanism for Web-Browsing Data:** The Commission recognizes the work that the DAA and the World Wide Web Consortium (W3C) have done in the area of Do Not Track, especially in the year between the proposed and final reports. The FTC is encouraged by the commitment of the industry, and hopes for full implementation of Do Not Track without the need for legislation. The Do Not Track mechanism must be easy to find, easy to understand, easy to use, comprehensive, effective and enforceable; and it must allow for universal implementation, and choices that are persistent and not easily overridden. In addition, Do Not Track should opt consumers out of collection of behavioral data for all purposes other than those consistent with the context of the consumer's interaction with the company.
- **Opt-In Consent for Material Retroactive Policy Changes & Sensitive Data:** Practices that require affirmative express consent include material retroactive changes to privacy representations and collection of sensitive data. "Sensitive" data includes information about children, financial and health information, Social Security numbers, and precise geolocation data.

Transparency

- **Shorter, Clearer, and More Standardized Privacy Notices:** The FTC recommends that the industry agree on standardized format and terminology for privacy notices. The FTC suggests that the multi-stakeholder meetings being convened by the DOC on privacy issues would be good places to discuss standardized format and terminology.
- **Proportional Access:** Consumer access to data should be proportional to the sensitivity and the intended use of the data at issue. For example, individualized access may not be feasible for data that is used only for marketing purposes. In that situation, entities should give consumers access to a list of the categories of data and the ability to suppress the use of such data for marketing. For entities using the data to make non-FCRA regulated eligibility decisions, consumers should have access to the types of information maintained and the source of such information to allow for correction of inaccuracies at the source.
- **Access to Teen Data:** Per the FTC, teens, who may act more impulsively than others when sharing data online, should be allowed to erase content posted online through a special eraser button mechanism. There has been much national and international conversation about a young person's "right to be forgotten," and the FTC generally supports such a right, but notes that an eraser button feature must be carefully crafted to protect First Amendment rights.
- **Special Consideration for Data Brokers:** The FTC, asserting the special nature of the so-called data broker industry, and the fact that consumers rarely are familiar with the practices of data brokers, recommends a centralized website where data brokers could identify themselves to consumers and provide information about how they collect and compile data. In addition, the FTC continues to support legislation giving access rights to consumers for information held by data brokers.

International Interoperability

The FTC set the framework in the context of other efforts being made around the world "to re-examine current approaches to protecting consumer privacy," namely:

- Asia Pacific Economic Cooperation (APEC) member economies (including the United States) are currently working to implement a cross-border, privacy-rules system to facilitate data transfers among APEC members
- In November 2011, the Organization for Economic Cooperation and Development (OECD) launched a comprehensive review of its groundbreaking 1980 Privacy Guidelines in light of the momentous technological changes over the past 30 years
- On January 25, 2012, the European Commission published its proposal for a Data Protection Regulation intended to overhaul and replace the European Data Protection Directive 95/46/EC. Implementation through a Regulation rather than a Directive is intended to deliver greater consistency and harmonization than has been achieved through national laws implementing the Directive. The Regulation is expected to come into force across the European Union within the next three years.

While the prospects of increased global interoperability and convergence are difficult to predict, the framework contains a number of well-established elements of current European data protec-

tion law (including transparency/fairness principles, data minimization and quality principles, and increased control for individuals). The principles of Accountability and Privacy by Design are new stand-out aspects of the proposed EU Data Protection Regulation. In addition, the wider scope of personal information proposed by the FTC is more in line with the European concept of "personal data", including information that can be used to indirectly identify an individual. As such, we can at least say that, at the highest level, the thinking of lawmakers and regulators on both sides of the Atlantic is converging.

Dissenting Statement of Republican Commissioner Rosch
Many of the most interesting statements within the Final Report come from the dissent of Republican FTC Commissioner J. Thomas Rosch.
Rosch agrees with certain recommendations of the Final Report, such as the recommendation that Congress enact legislation targeted at data brokers, as well as federal legislation requiring entities to maintain reasonable security and have data breach notification obligations. However, he voices his concern that the FTC may be overstepping its boundaries with the Final Report. Rosch warned, "If implemented as written, many of the Report's (sic) recommendations would instead apply to almost all firms and to most information collection practices … It would install 'Big Brother' as the watchdog over these practices not only in the online world but in the offline world."

If Rosch's major concerns over the Final Report are any indication of industry doubt, the FTC may need to work a bit harder to persuade the major players in the technology industry to join in with its voluntary regulatory proposals. Namely, Rosch is concerned that the Final Report's future harm indications are rooted in the "unfair" prong, rather than the "deceptive" prong of section 5, and that "unfairness" is an "elastic and elusive concept." To this extent, he expresses doubt that "reputational harm" should be considered a type of harm that the FTC should redress, while pointing out that the FTC has not generally enforced section 5 against intangible harms and has represented to Congress that it would not do so. If a standard does start to emerge where "reputational harms" are redressable, then one can't help but wonder what effect this might have in the context of privacy class actions, where claims based upon "reputational harms" have traditionally not been recognized in courts.

Rosch also expressed antitrust concerns over Do Not Track - major browser firms may act strategically and opportunistically to use privacy to protect their own entrenched interests. Rosch says he is unsure whether all the interested players in the arena would be able to come to agreement about exactly what Do Not Track means and what it entails.

Our team of privacy attorneys will be carefully monitoring further interpretations of the FTC's Final Report as companies begin to implement the FTC's recommendations. If you have any questions regarding the teleseminar or the content of this alert, please contact any of the authors of this post, or the Reed Smith attorney with whom you normally work.

About Reed Smith

Reed Smith is a global relationship law firm with nearly 1,700 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.