FTC Needs Industry Privacy Guidance for New Report

December 16, 2010

Mark Melodia | Christopher Cwalina | Paul Bond | Amy Mushahwar

ReedSmith

The business of relationships.

Introduction - Preliminary FTC Staff Report – released 12/1/10

- **"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."**
- Within every business, privacy should be a basic consideration – similar to keeping track of costs and revenues, or strategic planning.
- "While recent announcements of privacy innovations by a range of companies are encouraging, many companies – both online and offline – do not adequately address consumer privacy interests."
- "Industry must do better."
- The report proposes a framework for how companies should protect consumers' privacy.
- It is intended to inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines.
- The framework is designed to serve as a policy vehicle for approaching privacy, but it includes elements that reflect long-standing FTC law.

Introduction (continued)

- In introducing the proposed framework, the report discusses the FTC's Privacy Roundtables and major themes:
  - the ubiquitous collection and use of consumer data;
  - consumers' lack of understanding and ability to make informed choices about the collection and use of their data;
  - the importance of privacy to many consumers;
  - the significant benefits enabled by the increasing flow of information; and
  - the blurring of the distinction between PII and supposedly anonymous or de-identified data.
- The report highlights perceived **inadequacies** in the current **notice-and-choice and harm-based models of privacy,** saying that these models, while still relevant, have led to:
  - long, incomprehensible privacy policies that consumers typically do not read or understand;
  - and have not recognized a wider range of privacy-related concerns, including reputational harm or the fear of being monitored or simply having private information "out there."

Introduction (continued)

- Report highlights FTC's historical and recent privacy initiatives, i.e., FTC's efforts in areas of enforcement, consumer/business education, policymaking and research, and international activities
- FTC also points to the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers.
- Finally, the FTC says that industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection.

The Proposed Framework: Scope

- Very broad – beyond the existing sector-specific legal framework.
- Would apply to all online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device.
- Would apply regardless of whether such entity interacts directly with consumers.
- The report casts severe doubt on claims that de-identified information need no protection, citing to multiple instances and methods by which PII can be mined from seemingly anonymous information, which do not include names (instead, IP Addresses or other unique identifiers). The distinction between PII and non-PII is, the report says, "of decreasing relevance“.

The Proposed Framework: Components

- Privacy by Design
- Consumer choice
- Transparency

ReedSmith

The business of relationships.

Privacy by Design

- Companies should build privacy protections into their everyday business practices, including providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy.
- Companies should maintain comprehensive data management procedures throughout the lifecycle of their products and services.
- Companies should enforce procedurally sound privacy practices, such as assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services.

Consumer Choice – Reducing the Consumer's Information Burden

- Companies need to reduce the information burden on the consumer as presently it is the consumer's responsibility to understand company information practices.
- The FTC hopes to increase consumer digital literacy by providing more streamlined choices to consumers about their data practices, combined with government and private consumer education to demystify information privacy.
- **What can be streamlined?** Choice is not necessary for a limited set of **commonly accepted practices** – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. This includes sharing of consumer data with service providers acting at their direction for these purposes provided there is no further use of the data.

ReedSmith

The business of relationships.

Consumer Choice (continued)

- **What should remain?** For **non-commonly accepted practices**, choices should be clearly and concisely described and offered when – and in a context in which – the consumer is making a decision about his or her data. The consumer's decision should be durable.
  - Data collection across websites, even if done by a single party and not shared with others, will in some cases take a data practice out of the category of commonly accepted practices and require notice and choice
  - The FTC cited as an example of this deep packet inspection by ISPs.
- **Do Not Track Mechanism Supported.** Staff also supports universal choice options such as a "Do Not Track" capability (likely through a persistent setting on a consumer's browser) where consumers could choose whether to allow the collection and use of data regarding their online searching and browsing activities.

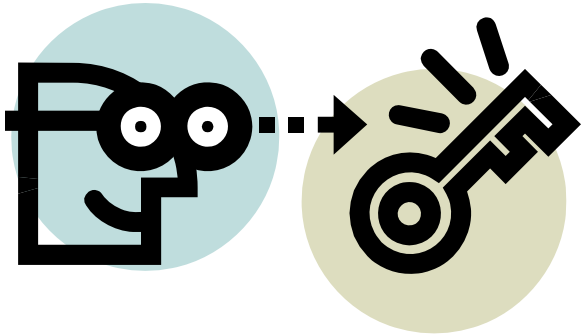
Transparency

- Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices. *(The FTC cited to the standardized GLBA forms, but industry is still determining whether these safe harbor forms are effective.)*
- Companies should provide **reasonable access** to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.
- Companies must provide prominent disclosures and obtain **affirmative (opt-in) express consent** before using consumer data in a materially different manner than claimed when the data was collected.
  - FTC states this is based on well-settled FTC case law and policy, and this concept was also contained in the final Behavioral Advertising staff guidelines.
- All stakeholders should work to educate consumers about commercial data privacy practices.

Additional Themes

Opt-in vs. Opt-out is Less Important, the Goal is Consumer Understanding:

- The report does not support opt-in or opt-out as the means for informed consent but instead discussed that clear, simple and prominent opt-out mechanisms may be more privacy protective than confusing, opaque opt-ins.
- The time and effort required for consumers to understand and exercise their options may be more relevant to the issue of informed consent than whether the choice is technically opt-in or opt-out.



Additional Themes (continued)

Further Clarifications Necessary for Mobile Services:

- Downloaded apps on mobile services is listed as an example of where all companies involved in information collection and sharing must provide meaningful choice mechanisms to customers. Vladeck mentioned this week that is was 'astounding' that one mobile provider's privacy policy that he viewed was 134 pages on the mobile device.
- Among the areas for comment: transparent notice and choice in the mobile environment and the difficulties presented by small screens, whether certain sensitive data or sensitive users warrant additional protections, and whether deep packet inspection would warrant enhanced consent or even more heightened restrictions because of the scope of information collected and the inability of many consumers to discontinue broadband service.

Concurring Statement of Commissioner Kovacic (R)

- While concurring with release, does not endorse its content or perspective as now presented.
- Proposal for a Do-Not-Track system is premature.
- Wants more context about or fuller review of:
  - the existing framework for federal and state oversight of privacy;
  - legal concepts (tort, property, contract law) that underlie privacy policy and doctrine;
  - modern literature on consumer's valuation of privacy.
- This report differs from earlier reports in proposing an expanded concept of harm but it does not address how the FTC's application of the harm test has developed in practice.
- Proposes additional questions for comment primarily about default terms and the consequences and enforcement of a Do-Not-track mechanism.

Concurring Statement of Commissioner Rosch (R)

- Commissioner Rosch finds the report to be flawed and argues that a new framework is unnecessary.
- He points out that the FTC has never challenged a company's failure to offer a particular kind of choice, suggesting that the answer is to enforce the notice model, not replace it with a new framework.
- Report alleges that surveys have shown that majority of consumers are uncomfortable with being tracked online; but it is in accurate to assert a majority of consumers feel this way.
- The appropriate remedy for opacity is to require notices to be clear, conspicuous and effective.

Concurring Statement of Commissioner Rosch (R) (continued)

- The Commission could overstep its bounds if it were to begin considering reputational harm or fear of being monitored or other intangible privacy interests. The Commission has specifically advised Congress that absent deception it will not enforce Section 5 against alleged intangible harm.
- With respect to the proposed opt-in requirement specifically pertaining to material changes, the report is ambiguous as to whether this requirement would apply no matter how clear and conspicuous the disclosure of the prospect of material change was. There may be no warrant for requiring more than an opt-out requirement if that was what was initially required, when the disclosure of the material change and the ability to opt-out is made clearly and conspicuously and the consumer actually receives the notice.

Timeline

- Commission staff seeks comment by January 31, 2011, on each component of the proposed framework and how it might apply in the real world.
  - Appendix A: 50+ questions
  - Plus additional questions posed by Commissioner Kovacic
- Interested parties are encouraged to raise, and comment upon, related issues.
- Based on comments received, the Commission will issue a final report in 2011.
- In the meantime, the Commission plans to continue its vigorous law enforcement in the privacy area, using its existing authority under Section 5 of the FTC Act and other consumer privacy laws it enforces (GLBA, COPPA, CAN-SPAM, and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Do Not Call Rule").

What Will Become Of This?

- **Preliminary Report:** The existing report requests public comments.
  - Comments deadline January 31, 2011.
  - *Ex parte* meetings may occur after this deadline.
- **"Final" Staff Report:** Vladeck stated earlier this week that he expects a final staff report to be issued in June or July of 2011.

ReedSmith

The business of relationships.

What Will Become Of This? (continued)

Procedural Unknowns: A few undetermined procedural questions include the following:

- Other Agency Buy-in: for telecommunications companies, national banks and other companies that are exempt from FTC regulation in many instances, the FTC must liaise with agencies such as the FCC or OCC, for example, how will the streamlined notice and transparency concepts jell with the FCC's CPNI rules?
- Legislative / Regulatory / Self Regulatory Implementation: for each proposal it has yet to be determined the level of implementation necessary. In particular,
  - Do Not Track: legislative, regulatory and self regulatory options are all on the table. In the Rush hearing last week, Rep. Markey announced he will be introducing a "Do Not Track" bill. Rush also likely to reintroduce his Best Practices Act with "Do Not Track" verbiage. Most Republicans in the hearing also supported a "Do Not Track" concept in practice.
  - Standardized Policies: regulatory (multi-agency coordination may be necessary to address universe of entities) and self-regulatory
  - Mobile Streamlined Policies: regulatory (with FCC coordination) and self-regulatory.

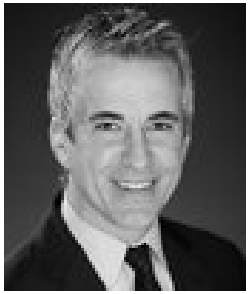
ReedSmith

The business of relationships.

Our Team

Mark Melodia
+1 609 520 6015
mmelodia@reedsmith.com

Mark leads the Global Data Security, Privacy & Management practice as a partner within the Global Regulatory Enforcement Group. Mark has led defense efforts in more than sixty putative class actions arising from alleged consumer privacy violations. Consumer privacy events often attract the attention of public actors. In that connection, Mark routinely represents clients responding to government privacy investigations, including before the Federal Trade Commission, the Office for Civil Rights, the State Attorneys General, and the United States Department of Justice. Overall, Mark has defended more than 150 class and 100 mass actions. This practice has taken him to trial and appellate courts in 24 states from Maine to Washington, and from Florida to California. Arbitration and mediation are also methods of dispute resolution in which Mark regularly engages.



Christopher Cwalina
+1 202 414 9225
ccwalina@reedsmith.com

Chris is in Reed Smith's Washington, D.C., office. Chris has extensive experience in the data privacy and information security. He has advised corporations on regulatory issues and legislative affairs and has provided counsel on compliance with GLBA, HIPAA, FCRA, COPPA, FCPA, and international privacy rules including the Data Protection Act. Chris also has experience developing in-house policies and procedures, including Information Security, global compliance matters, compliance frameworks and training. Prior to joining Reed Smith, Chris was Vice President and Associate General Counsel with Intersections Inc. Prior to that, Chris was employed with ChoicePoint Inc., Bayer Corporation and The Dow Chemical Company.

ReedSmith

The business of relationships.

Our Team

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

Paul is a member of the Global Regulatory Enforcement Group, practicing in the areas of data privacy, security, and management. Paul helps our clients comply with legal requirements for the protection of personal data, whether those requirements arise from contract, state, national, or international law. In that vein, Paul counsels clients on how to meet their obligations under, e.g., the Gramm-Leach-Bliley Act, HIPAA, the Fair Credit Reporting Act and its Identity Theft Red Flags regulations, and the dozens of other federal and state privacy law and regulations. Paul has also been actively involved in the successful defense of several dozen putative class actions concerning consumer privacy. Paul is a member of the International Association of Privacy Professionals.

Amy Mushahwar
+1 202 414 9295
amushahwar@reedsmith.com

Amy practices in the telecommunications field, in the areas of media, privacy, data security, and emerging technologies. She advises clients with matters pending before the Federal Communications Commission, National Telecommunications and Information Administration, U.S. Congress, Federal Trade Commission, and federal courts. Amy assists privacy clients with the development of risk management programs, and counsels clients in the information technology industry with the development of Service Level Agreement contracts. Amy serves as Co-Chair of the Federal Communications Bar Association's Privacy and Data Security Committee. Prior to her legal carrier, Amy worked as a technology consultant and owned/operated a technology consulting company.

ReedSmith

The business of relationships.