COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Global Privacy and Data Security

December 1, 2010

FTC ANNOUNCES PROPOSED FRAMEWORK FOR REGULATING CONSUMER PRIVACY

Today, the Federal Trade Commission released its long-awaited report on consumer privacy. This report follows the series of privacy roundtables that the FTC held over the past year. The FTC has invited comment on its proposals, which are due **January 31, 2011**. Based on comments received, the FTC has indicated that it will refine its proposal, issue a final report, and make legislative recommendations to Congress in 2011.

In remarks introducing the report earlier today, Consumer Protection Bureau Director David Vladeck emphasized the FTC's view that "self-regulation has not kept pace with technology." Today's report signals an effort to address that concern — and the perceived weaknesses in the FTC's historic approaches to privacy regulation — by providing a normative framework for how companies should protect consumers' privacy. It also reflects the agency's expectation that companies will do more immediately to protect privacy, including by enhancing their privacy disclosures and implementing more rigorous internal policies concerning data management.

Proposed Scope & Enforceability

Applies to:

- commercial entities
- involved in collection *or* use
- data that can be reasonably linked to an individual, regardless of whether the data is "personally identifiable"

The report endorses a privacy "framework" that is not limited to online practices or the collection of personally identifiable information. The framework would apply to all commercial entities --- whether operating online or offline and regardless of whether the entities have a direct relationship with consumers — that collect or use any data that "can be reasonably linked to a specific consumer, computer, or other device." The FTC seeks comment on the scope of its framework.

The FTC has not addressed directly the enforceability of the report's recommendations, but it is reasonable to anticipate that the FTC may enforce those aspects of the final report that it concludes are within its authority under Section 5 of the FTC Act or other statutes. FTC Chairman Jon Leibowitz indicated in a prepared statement that the agency would use its new framework to inform enforcement actions under its existing legal authority, "especially when children and teens are involved."

Proposed Principles

Three Core Principles

The FTC's proposed regulatory framework is based three core principles: privacy by design, choice, and transparency.

Privacy By Design

- privacy at every level of the organization
- incorporate privacy into product development
- adopt comprehensive data management procedures

In the report, the FTC finds that privacy should be an integral part of a company's processes for developing products, a concept that the FTC calls "privacy by design."

For example, the report encourages companies to adopt and enforce practices to limit data collection, protect data that is collected, implement reasonable data retention periods, and ensure that consumer data is accurate. The framework also urges companies to adopt privacy principles throughout their organizations, including through training and by appointing personnel with responsibility for overseeing ongoing privacy compliance reviews. The FTC seeks comment on the specifics regarding these proposed requirements.

Choice

- provide "just-in-time" disclosure and choice at the time of collection or use
- choice not required for "commonly accepted" practices — e.g., fulfillment, legal, product improvement
- first-party marketing deemed "commonly accepted" but not third-party marketing

The FTC's approach would require companies to offer consumers choices for data practices that do not constituted "commonly accepted practices" as defined by the FTC. Specifically, the FTC would not require companies to provide choices to consumers about the collection and use of consumer data for product and service fulfillment, internal operations such as product improvement, fraud prevention, legal compliance, and first-party marketing. One focal point for comments on the report is likely to be whether this proposed list of "commonly accepted practices" is too narrow or too broad and how these practices, including most specifically first-party marketing, will be defined.

For all other data practices, the report calls on businesses to offer consumers clear and prominently disclosed choices. The FTC envisions that companies will offer these choices at the time and in the context in which the consumer is making a decision about his or her data. For example, the FTC suggests that an online retailer will provide a clear and conspicuous disclosure and control mechanism on the page on which a consumer types in his or her personal information. The FTC indicates that choices within "long" privacy policies and "pre-checked boxes" are ineffective.

The report does not express a preference for "opt in" versus "opt out" consent but seeks comment on the appropriate form of consent, including whether the method should vary by context. The report does suggest, however, that enhanced protections — in the form of affirmative express consent — are appropriate for sensitive data, which the FTC defines as including information about children, financial and medical information, and precise geolocation data.

Choice *(continued)*

- browser-based "do not track" endorsed
- browser would notify site not to track or use collected data for targeting
- asks whether more granular controls should be offered
- FTC seeks enhanced enforcement authority

For online behavioral advertising, the report endorses the development of a "do-not-track" framework as a key option for implementing a robust consumer choice framework. The report suggests that uniform choice might be implemented through a persistent browser setting that would inform websites not to track a user or use behavioral information about the user for targeting purposes. The FTC acknowledges that its do-not-track approach cannot be effective unless sites have an enforceable obligation to honor user preferences. But the FTC nonetheless believes that this approach is preferable to current cookie-based approaches, which consumer groups have criticized as under-inclusive and vulnerable to manipulation, and to "registry-based" approaches like the federal Do Not Call program, which it believes would not be technically feasible and could raise new privacy issues.

The FTC has invited comment on how a universal choice mechanism could work in practice and whether consumers should be given more granular choices regarding tracking and targeting. The report also acknowledges that the FTC does not have the authority to impose a "do-not-track" mandate today, but Director Vladeck indicated today that the agency may attempt to "coax and cajole" implementation even as it seeks comment on whether to request broader enforcement authority from Congress.

Transparency

- existing privacy policies not enough
- standardization of disclosures
- reasonable data access
- prominent notice and consent for material, retroactive changes
- consumer education

The report also calls for privacy policies that are shorter, clearer, and more standardized. The FTC seeks comment on how to best ensure the usability and comprehension of privacy notices, requesting specific comment on the feasibility of standardizing the format and terminology across industries. By encouraging more consistent privacy policies and "at a glance comparisons," the FTC hopes to encourage companies to compete on the basis of their privacy practices.

The FTC's framework also pushes for increased consumer access to information held about them by data aggregators and other entities with which they do not do business directly. Further, the FTC calls for all stakeholders to expand their efforts to provide consumer education about commercial data privacy practices.

Consistent with the existing FTC approach, the report also makes clear that before making material changes to a privacy policy, a company should make prominent disclosures that clearly describe such changes and obtain consumers' affirmative consent.

* * *

The FTC's proposed privacy framework, if adopted, would require companies to modify their online and offline privacy practices in significant ways. We encourage companies to closely review the FTC's report, available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, and the list of questions posed by the FTC, which is attached below.

If you have questions regarding the FTC report or its impact on your business, or if you are interested in submitting comments, please contact the following members of our privacy and data security practice group:

Erin Egan	202.662.5145	eegan@cov.com
Yaron Dori	202.662.5444	ydori@cov.com
Rob Sherman	202.662.5115	rsherman@cov.com
Lindsey Tonsager	202.662.5609	ltonsager@cov.com
Libbie Canter	202.662.5228	ecanter@cov.com
Josephine Liu	202.662.5654	jliu@cov.com
Steve Satterfield	202.662.5659	ssatterfield@cov.com

Appendix to FTC Report

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?