Privacy Alert

FTC's Proposed Framework for the Protection of Consumer Privacy: A Signal of Expanded Regulation and FTC Oversight?

MICHAEL R. EGGER

Fenwick
FENWICK & WEST LLP

On December 1, 2010, the Federal Trade Commission (**"FTC"**) released a report entitled "Protecting Consumer Privacy in an Era of Rapid Change" (the **"FTC Report"**), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. The FTC Report, which proposes a new framework for protecting consumer privacy, is intended to inform policymakers, as they develop policies and enact privacy-related laws, and to guide and motivate businesses, as they develop and implement best practices and self-regulatory guidelines. The FTC Report raises numerous very interesting and complex policy and practical questions for which the FTC is seeking comment by January 31, 2011. The FTC intends to issue a final report later this year.

CONCERNS WITH EXISTING PROTECTION OF CONSUMER PRIVACY

While acknowledging that companies are using consumer information in new ways to make available innovative products and services, and that many of these companies manage consumer information responsibly, the FTC Report expresses concern that some companies appear to treat consumer information in an irresponsible or reckless manner. The FTC Report describes the myriad ways in which information regarding consumers' purchasing behavior, online browsing habits and other activities is collected, analyzed, combined, aggregated, used and shared. Although the FTC Report acknowledges that some consumers may be aware of these practices and accept them as a tradeoff for access to innovative products and services, the FTC Report cites concern for those consumers who may not be fully aware of the extent to which discrete items of their information are shared, compiled and aggregated, and for those consumers who fail to understand and appreciate the potential consequences and risks arising from these practices.

SCOPE OF PROPOSED FRAMEWORK

The proposed framework would apply to all commercial entities that collect, maintain, share or otherwise use consumer information that can be reasonably linked to a specific consumer, computer or other device, even if the consumer information does not constitute what would traditionally be considered personally identifiable information (**"PII"**). The broad scope derives in part from the continuing loss of a distinction between PII and non-PII, resulting from technology changes and the ability to re-identify consumers from supposedly anonymous data. The broad scope is designed to encompass both online and offline entities that collect consumer information, regardless of whether such entities directly interact with consumers. The FTC Report acknowledges that further thought needs to be given to defining exceptions from the framework for certain types of businesses, e.g., businesses that collect, maintain or use a limited amount of non-sensitive consumer information.

COMPONENTS OF PROPOSED FRAMEWORK

The proposed framework consists of the following three components:

- **Privacy by Design:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.
- **Simplified Choice:** Companies should simplify and streamline the manner in which they provide choices to consumers as to the collection, use and sharing of their information.
- **Greater Transparency:** Companies should increase the transparency of their practices with respect to the collection, use and sharing of consumer information.

PRIVACY BY DESIGN

The FTC Report urges companies to incorporate certain substantive privacy and security protections into their routine business operations and to consider privacy issues at all stages of the development of their products and services. These privacy and security protections are based on the following four principles:

Reasonable Safeguards. Companies should employ reasonable safeguards to protect the consumer information that they maintain, including physical, technical and administrative safeguards. What safeguards are appropriate would depend on the sensitivity of the information, the size and nature of a company's business operations, and the types of risks a company faces.

Scope of Collection. Companies should give due consideration to their information collection practices to ensure that they collect only the information needed to fulfill a specific, legitimate business need. Limiting the scope of collection decreases the risk of unauthorized access as well as the potential harm that could result from such access.

Data Retention. Companies should implement reasonable and appropriate data retention periods so that they store consumer information only for as long as they have a specific and legitimate business need to do so. Having more reasonable and appropriate retention periods is intended to mitigate the risk of companies using stored information in ways that consumers did not anticipate when they provided the information, and to reduce the attractiveness of databases of consumer information as targets for identity thieves.

Data Accuracy. Companies should take reasonable steps to ensure the accuracy of the data they collect, particularly if such data could be used to deny consumers benefits or cause significant harm. For example, some data brokers sell identity verification services to both public and private entities, and if any such data is erroneous and does not match the identifying information presented by a consumer, the consumer can suffer economic or other harm.

To ensure that these four principles are properly incorporated into their business models, the FTC Report urges companies to develop and implement comprehensive privacy programs and to designate specific personnel with responsibility for employee privacy training and for promoting accountability for privacy policies throughout the organization. Companies should also conduct periodic reviews of their internal policies to address changes in their business or other privacy-related developments that may require modifying their practices or privacy policy. The FTC Report indicates support for the use of identity management, data tagging tools, Transport Layer Security/Secure Sockets Layer or other privacy-enhancing technologies to establish and maintain strong privacy policies.

SIMPLIFIED CHOICE

The FTC Report urges companies to present choices to consumers regarding the collection, use and sharing of their information in a simpler and more streamlined manner. For certain common business practices that are deemed to be obvious from the context of the transaction or that are sufficiently accepted or necessary for public policy reasons, "simplified choice" actually means that companies need not request consent from consumers to engage in them. These common business practices, referred to as "commonly accepted practices," are as follows:

Product and Service Fulfillment. Websites routinely collect consumers' contact information and credit card payment information in order to process and fulfill consumers' orders.

Internal operations. Hotels and restaurants collect customer satisfaction surveys to improve their customer service. Websites collect information about visits and click-through rates to improve site navigation.

Fraud prevention. Retailers' efforts to prevent fraud include checking drivers' licenses, employing fraud detection services and scanning ordinary web server logs.

Legal compliance and public purpose. Search engines, mobile applications, and pawn shops share their customer data with law enforcement agencies in response to subpoenas. Businesses report a consumer's delinquent account to credit bureaus.

First-party marketing. Retailers recommend products and services based upon consumers' prior purchases on the website or at an offline retail store.

As to all other business practices for which consumer consent is required, the FTC Report urges that choices be presented clearly and concisely, taking into account that both the context and the timing of presenting

choices have an impact on consumer understanding. For companies with relationships with consumers, e.g., online retailers, choices should be presented when the consumer is requested to provide any personal information. The FTC Report queries whether some form of enhanced consent should be required for sensitive information and sensitive users, e.g., requiring affirmative express consent from children, particularly teens, and for financial and medical information and precise geolocation data. The FTC Report addresses the challenges of ensuring that consumers have meaningful choice with respect to the collection of information by companies that do not directly interact with consumers. These companies, commonly referred to as information or data brokers, may be unable to present choices at the point of collection or use of consumer information. The FTC Report also devotes considerable attention to the high-profile issue of behavioral advertising. Although it acknowledges the development of certain tools to enable consumers to better control the use of their information for behavioral advertising, and efforts by industry to develop self-regulatory guidelines and an opt-out mechanism for behavioral advertising, the FTC Report states that efforts to implement an effective mechanism for choice on an industry-wide basis have fallen short. Consequently, the FTC Report indicates support for a more uniform and comprehensive mechanism, sometimes referred to as "Do Not Track." As conceived, this mechanism would involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted advertisements.

Greater Transparency

The proposed framework calls for several measures directed at making more transparent to consumers companies' practices with respect to the collection, use and sharing of consumer information. Specifically, in order to improve the ability of consumers to compare practices across companies, the FTC Report calls for companies to make privacy policies more uniform, perhaps using standardized forms and terminology, much shorter in length, and written more simply in a manner that consumers will be better able to understand. The FTC Report also urges companies to provide consumers with reasonable access to their information, while acknowledging that requiring such access raises concerns as to the cost of providing access, the ability of companies to authenticate the identity of consumers requesting access, and the potential privacy threats of requiring access.

In order for companies' efforts to provide consumers with simplified choice and greater transparency to be meaningful, companies must provide prominent disclosure and obtain express affirmative consent for any material changes to their privacy policy that would apply retroactively to any information previously collected. Finally, it is proposed that stakeholders undertake accelerated efforts to educate consumers about commercial data practices and the choices available to them.

Conclusion

The FTC Report raises some very complex policy and practical issues regarding consumer privacy. Those companies whose businesses rely on the collection, compilation, aggregation, sharing or use of consumer information should closely track the FTC's further development of the proposed framework as the FTC considers input and feedback from individual businesses, industry, consumer groups, academics and government. It seems likely that some changes are imminent, some of which may be significant.

For more information about this article, please contact:
Michael R. Egger (megger@fenwick.com)
Jennifer Stanley (jstanley@fenwick.com) or
Stefano Quintini (squintini@fenwick.com) of Fenwick & West LLP.