WHITE & CASE

Articles

New FTC Report Recommends Changes to United States Privacy Law

April 18, 2012
Daren M. Orzechowski, Allison M. Dodd

Technology Newsflash

On March 26, 2012, the Federal Trade Commission ("FTC") issued its final report on consumer privacy in the United States, entitled Protecting Consumer *Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (the "FTC Privacy Report").[1] The purpose of the FTC Privacy Report is to provide companies that collect and use consumer data with an outline of best practices to implement for dealing with consumers' personal information. Another purpose is to encourage enactment of and provide guidelines for Congress when considering enactment of baseline and other targeted privacy legislation.[2] The FTC Privacy Report, however, "is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC."[3] Instead, it is meant to inspire and provide guidelines for change in how privacy and data protection matters are handled within the United States. Until Congress enacts legislation or regulations, or companies volunteer to self-regulate, the FTC Privacy Report merely outlines best practices for companies and businesses and does not provide the basis for legal actions.

The FTC Privacy Report reflects the FTC's final conclusions concerning current consumer privacy protections in the United States, initially described in the preliminary staff report, entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (the "Proposed Framework"), published in December 2010 and previously discussed in one of White & Case's earlier Technology Newsflash posts.[4] Although much of the FTC Privacy Report mimics the Proposed Framework and previous statements of the Obama Administration, the current report includes notable revisions as a result of the FTC's numerous roundtable discussions and over 450 comments submitted from businesses, academics and consumers following the issuance of the Proposed Framework.

The Current FTC Privacy Report

Similar to the Proposed Framework, the FTC Privacy Report outlines best practices for companies that collect, use, and share consumer data (online or offline) that can be "reasonably linked to a specific consumer, computer or other device."[5] The report focuses on the following three elements of data privacy.

- Privacy by Design: The FTC urges companies to implement substantive privacy protections that are tailored to their specific businesses. Substantive protections include reasonable data security measures, reasonable data collection limits, sound data retention and disposal practices, and steps to maintain reasonably accurate consumer data.[6] The FTC Privacy Report recommends that companies develop and maintain procedures to implement these protections throughout the life cycle of their products and services.[7]
- Simplified Consumer Choice: The Proposed Framework recommended that companies provide consumers with "easy-to-use choice mechanisms that allow consumers to control whether their data is collected and how it is used."[8] The FTC Privacy Report further provides that companies do not need to provide consumer choice prior to collection and use of consumer data in a manner consistent with the context of a transaction, a company's relationship with the consumer, or as required by law. For practices inconsistent with the context of a company's interaction with consumers, the FTC recommends that companies provide consumers with a choice mechanism at a time and in a context relevant to the consumer's decision concerning whether to allow collection or use of his or her personal information.[9] Although this determination is fact-specific, generally a company should provide consumers with this choice at or immediately before the time the company collects the consumer's information.[10] In addition, the FTC reiterates its support for the implementation of a universal "Do Not Track" mechanism, a choice mechanism for online behavioral advertising that would allow consumers to limit the tracking of their online activities.[11]

- Transparency: In order to increase consumer awareness of how, why and what kinds of information companies collect, the FTC Privacy Report recommends that companies improve transparency of their data practices.[12] Privacy notices should be clear and concise statements describing a company's data collection and use practices and should contain standardized terminology in a consistent format to increase consumer understanding and enable consumers to effectively compare privacy policies of competing companies.[13] In addition, companies should provide reasonable access to their stored consumer data, in proportion to the sensitivity of the data collected and the companies' use of the data, and expand their efforts to educate consumers about commercial data privacy practices.[14]

Notable Changes from the Proposed Framework

The FTC Privacy Report makes some noteworthy changes to the Proposed Framework. The major differences between the two reports are that the FTC: (1) alters the scope of the report from its initial proposal in the Proposed Framework, (2) revises the standard for when to provide consumers with a choice mechanism concerning the collection and use of their information, and (3) recommends that Congress enact baseline privacy legislation and specific legislation to address the data collection and use practices of information brokers.

(1) Scope

In the FTC Privacy Report, the FTC limits the types of entities that would be subject to the review and action suggested in the Proposed Framework in order to avoid unduly burdening small businesses. Now, the FTC recommends that entities that collect limited non-sensitive consumer data from fewer than 5,000 consumers, and do not share such data with third parties, should not need to comply with the proposed regulation, assuming of course that the proposals are enacted into law.[15]

The report also narrows the types of data proposed to be covered in the Proposed Framework. In the Proposed Framework, the FTC recommended that companies must take steps to protect data that can be "reasonably linked to a specific consumer, computer, or other device."[16] In response to public comments expressing concern that more data may increasingly be "reasonably linked" to consumers as technology advances, the FTC in the FTC Privacy Report excludes such data from proposed protection where a company complies with three requirements. First, the company must take reasonable measures to ensure that the data is de-identified. In doing so, the company must have a "reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer or other device."[17] Second, the company must commit publicly to maintain and use the data in a de-identified fashion. Third, if the company makes de-identified data available to third parties, it must contractually prohibit all third party recipients from attempting to re-identify the data.[18]

(2) Simplified Consumer Choice

In the FTC Privacy Report, the FTC alters the proposed standard for when to provide consumers with an option to share (or not share) their personal information. In the Proposed Framework, the FTC explicitly listed five categories of data that companies could collect and use without offering consumers a choice of opting in or out of the collection. The FTC noted that data collection in these circumstances was either obvious or necessary for public policy reasons. These categories included personal information used by the collecting company for: (1) product and service fulfillment, (2) internal operations, (3) fraud prevention, (4) legal compliance and public purpose, and (5) first-party marketing.[19] The FTC changes its approach in the current FTC Privacy Report, and now implements a "context of the interaction" standard. The determination of whether a consumer must be given a choice to opt out of collection of his or her personal information now "turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[20]

The FTC believes that when a company uses consumer information for purposes that are inconsistent with the context of their interaction with the consumers, companies should give consumers a choice of whether to allow collection or use of their data, at a time and in a context relevant to making the decision concerning use of their data.[21] Conversely, companies do not need to provide consumers with a choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer.[22] In all circumstances, however, companies should obtain express affirmative consent: (1) before using consumer data in a manner materially different than described in privacy representations in effect at the time the data was collected and (2) before collecting sensitive data (including information about children, financial and health information, social security numbers, and precise, individualized geolocation data).[23] Such concepts are not unique as some of these principles exist under European data privacy law.

(3) Future Legislation

It is important to note that the FTC Privacy Report does not have the force of law yet. The report is not legislation, but rather a series of proposals. In the FTC Privacy Report, the FTC urges Congress to consider enacting baseline privacy legislation, in order to increase transparency of businesses' data sharing practices.[24] In addition, the FTC recommends that Congress

enact targeted legislation to allow consumers to access their data as collected and maintained by information brokers and to otherwise increase transparency and disclosure of the practices of information brokers.[25]

Future FTC Action

Industry self-regulation and non-legislative measures have not disappeared from the discussions concerning American privacy law. The FTC Privacy Report notes that in the upcoming year, the FTC will be especially active in the following areas of privacy law.

- Do Not Track Legislation: The FTC will work with the Digital Advertising Alliance and the World Wide Web Consortium to complete implementation of a universal, easy to use, persistent, effective and comprehensive Do Not Track system that allows consumers to opt out of collection of behavioral data for all purposes inconsistent with the context of the consumer's interaction with a company.[26]
- Mobile: The FTC recommends that companies providing mobile services develop short, meaningful privacy protection disclosures, while acknowledging the difficulties of navigating privacy matters in the context of mobile technology. The FTC initiated a project to update its business guidance about online advertising disclosures and will host a related workshop on May 30, 2012 that will address mobile privacy disclosure issues.[27]
- Data Brokers: The FTC challenges data brokers to increase transparency and consumer understanding by creating a centralized website where data brokers would: (1) identify themselves to consumers and describe how they collect and to whom they sell consumer data, and (2) detail the access rights and choices that consumers have with respect to the data collected by data brokers.[28]
- Large Platform Providers: The FTC intends to host a public workshop in the second half of 2012 to facilitate education concerning and discussion of heightened privacy concerns specific to large platform providers, such as ISPs, operating system and browsers and social media companies that have the ability to comprehensively track consumers' online activities.[29]
- Promoting Enforceable Self-Regulatory Codes: The Department of Commerce, with the support of stakeholders and the FTC, is working to facilitate the development of sector specific, self regulated codes of conduct.[30] The FTC commits to consider adherence to any strong privacy self regulatory schemes in its enforcement actions and to continue to bring enforcement actions against companies that engage in unfair and deceptive practices, including violations of self regulatory codes of conduct.[31]

Conclusion

As evidenced by the FTC Privacy Report and the White House's increased interest, consumer data privacy continues to garner significant attention. While it still appears to be a challenge for Congress to pass meaningful privacy legislation, proposals for regulation will continue to develop as a result of initiatives such as the FTC Privacy Report. Companies should continue to develop their privacy policies and practices to anticipate what appear to be likely legal changes.

To keep ahead of such changes, companies should regularly assess their privacy policies and disclosures to consumers and monitor the proposals that are being made. Companies should ensure that their privacy policies: (1) are consistent with all aspects of their business operations and provide substantive protections for consumer data, (2) provide consumers with a simplified choice as to whether and how their personal information is collected and shared, both at the relevant time and in the relevant context, and (3) disclose the company's privacy practices in a simple manner to increase transparency and consumer understanding.

---

1 Federal Trade Commission, FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf ("FTC Privacy Report").
2 Id. at i-iii, 1.
3 Id. at 1.
4 Federal Trade Commission, Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
5 FTC Privacy Report at 22.
6 Id. at 24-30.
7 Id. at 30-32.
8 Id. at 35.
9 Id. at 48-50.
10 Id. at 50.

11 Id. at 52-55.
12 Id. at 60-61, 64.
13 Id. 61-64.
14 Id. at 64-72.
15 Id. at 15-16.
16 Id. at 22.
17 Id. at 21.
18 Id.
19 Id. at 36.
20 Id. at 38-39.
21 Id. at 48-60.
22Id. at 38-39.
23 Id. at 57-60.
24 Id. at 11-13.
25 Id. at iv, 14, 69.
26 Id. at 52-55, 72.
27 Id. at 63-64, 73.
28 Id. at 69, 73.
29 Id. at 55-57, 73.
30 Id. at 73.
31 Id.
