Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

WSGR ALERT

MARCH 2012

FTC RELEASES FINAL PRIVACY REPORT, SETS FORTH BEST PRACTICES, AND CALLS FOR FEDERAL PRIVACY, DATA SECURITY, AND BREACH NOTIFICATION LEGISLATION

On March 26, 2012, the Federal Trade Commission (FTC) issued its long-anticipated final report on privacy, *Protecting Consumer Privacy in an Era of Consumer Change: Recommendations for Businesses and Policymakers*.[1] The final report comes more than a year after the FTC's preliminary staff report, which proposed a new framework for addressing privacy issues based upon three general principles: privacy by design, simplified choice, and greater transparency.[2] The final report represents the FTC's view as to best practices regarding consumer data and encourages the adoption of legislation and industry self-regulation. The FTC is the nation's leading consumer protection enforcement agency and has the authority to regulate all unfair and deceptive trade practices occurring in interstate commerce. The FTC has used this authority to assert jurisdiction over privacy-related matters for most businesses.

In its final report, the FTC largely retained its proposed three-principle framework, but it revised its recommendations in three key areas in response to public comments and commercial and technological developments: the scope of the framework, the contexts in which the framework calls for notice and choice to consumers prior to the collection and use of certain data, and the practices of data brokers. Specifically, the revised recommendations:

- clarify what information may be "reasonably linked to a specific consumer, computer, or other device," thereby falling within the framework, and provide a very narrow exception to the framework for small businesses that do not share the information they collect;
- exempt from the notice and choice requirement "practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law," replacing its five specific "commonly accepted" information collection and use practices that do not require notice and consent; and
- call for Congress to consider legislation governing the practices of data brokers regarding transparency and consumer control over the information collected.

The report also calls for federal privacy, data security, and data breach notification legislation, and urges industry to accelerate the pace of self-regulation to implement the framework.

Scope of Final Framework

The final framework, like the proposed framework, applies broadly to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device." This includes consumer information *collected or used* both online and offline. Thus, for example, the final framework applies to advertising networks that receive information from websites and mobile apps to facilitate targeted advertising, as well as brick-and-mortar establishments that sponsor consumer loyalty programs.

In response to concerns about the vagueness of the "reasonably linked" standard, the FTC clarified that data will not be deemed "reasonably linked" to a specific consumer, computer, or device if a company: (1) takes reasonable measures to ensure that the data is de-identified (i.e., the company has a "reasonable level of justified confidence" that the information cannot be used to infer information about or otherwise be linked to a specific consumer, computer, or device); (2) publicly commits to maintain and use the data only in a de-identified manner and not to try to re-identify it; and (3) contractually prohibits downstream data recipients from trying to re-identify the data.

Additionally, in recognition that the framework may place an undue burden on small businesses, the final framework does not apply to companies that (1) collect only non-sensitive information from fewer than 5,000 consumers a year and (2) do not share it with third parties.

---

[1] The full report is available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[2] See our WSGR Alert discussing the preliminary staff report at http://www.wsgr.com/wsgr/Display.aspx?SectionName=publications/PDFSearch/wsgralert_do_not_track_mechanism.htm.

Continued on page 2...

FTC Releases Final Privacy Report . . .

Continued from page 1...

Privacy by Design

The final report retains the FTC's proposed best practice that calls on companies to promote and incorporate substantive consumer privacy protections throughout their organizations and at every step in the process of developing their products and services. Among the substantive protections the FTC would like to see are reasonable security for consumer data, reasonable collection limits, and sound retention practices, as well as measures to ensure data accuracy.

The report calls upon industry to develop and implement "best data security practices" for the industry sectors and types of consumer data that have not been addressed already by self-regulation. It also calls upon Congress to enact data security and breach notification legislation authorizing the FTC to seek civil penalties for violations.

Regarding reasonable limits on data collection, the final report clarifies that, under the framework, companies should limit data collection to what is consistent with the context of the transaction or the relationship between the company and consumer, or what is required or specifically authorized by law. In other words, the FTC wants companies to consider whether their data collection is consistent with what a consumer reasonably would expect based on the context of the transaction or business relationship. Where the collection would not be consistent with consumer expectations at the time of collection, the framework encourages companies to provide prominent notice and choice to the consumer outside of a privacy policy or other legal document. In the FTC's view, companies should determine the purpose of any data collection prior to it taking place, and they should not collect data for possible future (but yet unknown) purposes. Companies also should satisfy the business purpose by collecting data that has the minimum potential privacy implications. The FTC applauded the use of palm prints rather than fingerprints to validate identity, for instance, because palm prints are less susceptible to "function creep," such as cross-referencing them against criminal databases.

With respect to data retention, the final report continues to set forth a best practice of limiting the retention of data and disposing of it once it has outlived the purpose for which it was collected. The FTC declined to define a specific data-retention period as a best practice, and instead the report calls for flexible procedures commensurate with a company's size and the risks associated with the data it collects, uses, and maintains.

The final framework, like the proposed one, continues to ask companies to take reasonable steps to ensure the accuracy of the data collected and maintained, particularly where the data could be used to cause significant harm or to deny services to consumers. The FTC adopted a flexible approach, calling for different requirements depending upon the intended use and sensitivity of the data. Under this approach, companies using consumer data for marketing purposes need not take special measures to ensure the accuracy of such data. However, companies using the data to determine a consumer's eligibility for benefits should take measures to ensure accuracy, including giving consumers access to the data maintained by the company and giving them the opportunity to correct it.

To implement these best practices, the final report continues to encourage companies to adopt and maintain comprehensive data-management procedures throughout their product or service lifecycles. These procedures may include designating privacy personnel responsible for training employees regarding privacy practices and conducting regular privacy assessments. The FTC pointed to the privacy programs required in its recent settlements with Google and Facebook as a "roadmap" to adequate data-management procedures.[3] The final report recommends a reasonable transition period for companies to update legacy systems to incorporate the privacy framework. It suggests that companies update systems with sensitive data first and appropriately limit access to such systems until they are updated.

Simplified Choice

The FTC retained simplified choice as a core component of its privacy framework. The preliminary report had proposed exempting from the notice and choice regime certain "commonly accepted" practices, such as order fulfillment, internal operations, fraud prevention, legal compliance, and most first-party marketing. The final report focuses instead on the *context of the interaction* between the consumer and the business, noting that the five "commonly accepted" practices generally will meet this standard. Under the FTC's revised principle, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or when the collection or use is required or expressly authorized by law.

The FTC specifically identified the sale of consumer information to a third party and the tracking of consumers across third-party websites as practices that *would* require notice and choice under the framework. Even the sharing of consumer data among affiliated companies should be disclosed, unless the affiliate relationship is clear to consumers. The report raises concerns about

[3]The privacy programs mandated by the FTC for Google and Facebook must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring. The WSGR Alert regarding Facebook's FTC settlement is available at http://www.wsgr.com/wsgr/Display.aspx?SectionName=publications/PDFSearch/wsgralert-facebook-ftc-settlement-privacy.htm.

Continued on page 3...

FTC Releases Final Privacy Report . . .

Continued from page 2...

"data enhancement,"[4] but recognizes that providing notice and choice prior to engaging in such a practice may not be feasible considering the costs and logistical problems it presents. Thus, the final framework relies upon privacy by design and transparency to address concerns about data enhancement.

The final report retains the notion that companies should provide notice and choice, when required, at a time and in a context in which the consumer is making a decision about his or her data. It clarifies, however, that precisely how companies practically achieve these goals may vary based on the circumstances. In some instances, notice and choice may be provided *after* data has been collected. For example, the report commends the online behavioral advertising industry's development of a standardized icon and text that is embedded into targeted advertisements because the in-ad disclosure provides a logical "teachable moment" for the consumer.

The report endorses obtaining affirmative, express consent from consumers before collecting sensitive data, such as information about children, finances, or health, regardless of the use of such data. Similarly, the report states that companies should obtain affirmative, express consent before making material, retroactive changes to privacy representations.[5] For the consumer's choice to be meaningful, the framework rejects a "take it or leave it" approach for important services where consumers have few options, such as broadband access.

The final report continues to advocate for the implementation of a "Do Not Track" mechanism that would give consumers choice with respect to online behavioral tracking. The report sets forth five key principles to make such a system effective.[6] It expresses concern regarding large platform providers, such as Internet service providers, operating systems, browsers, and social media companies, that can collect data comprehensively across the Internet, but it leaves that concern to be addressed at a later date.

Greater Transparency

The report reaffirms the FTC's proposed principle that companies should make privacy policies clearer, shorter, and more uniform so that consumers, regulators, and others more easily may compare policies among different companies. The FTC believes that uniformity can be achieved by industry sector.

The report also reaffirms the FTC's position that companies should provide consumers with reasonable access to the data about them that companies maintain. For data maintained for marketing purposes, the FTC concluded that the cost of providing individualized access and correction rights likely would outweigh the benefits. However, it endorsed the practice of companies providing consumers with access to a list of categories of data they hold, and the ability to opt out of its use for marketing. In contrast, businesses maintaining consumer data for use by creditors, employers, insurance companies, and others that make eligibility determinations with the data should provide consumers with individualized access to their own data and the ability to correct erroneous information. For companies that lie somewhere in the middle, the report endorses a sliding-scale approach; companies should adjust consumers' ability to access data about them based on the use and sensitivity of the data. The report asserts that, at minimum, companies should offer consumers access to (1) the types of information companies maintain about them and (2) the sources of such information.

Next Steps

The FTC's report calls for federal legislation in multiple areas and urges industry to accelerate the pace of self-regulation. Additionally, it specifically identifies five areas in which the FTC will focus its policymaking efforts this year:

- *Do Not Track.* The FTC intends to work with industry, browser vendors, the Digital Advertising Alliance, and the World Wide Web Consortium to implement an easy-to-use, persistent, and effective "Do Not Track" system.
- *Mobile.* The FTC will update its business guidance about online advertising disclosures to help companies with mobile services provide short, meaningful disclosures to consumers.
- *Data Brokers.* Of particular concern to the FTC are data brokers that combine consumer data from several sources and resell it, often without the consumer's knowledge. The FTC will advocate for targeted legislation requiring data brokers to provide consumers with access to information the broker holds about them. Further, the FTC recommends the creation of a centralized website where data brokers that use data for marketing can identify themselves to consumers and describe how they collect and sell consumer data. The website also could educate consumers on their access rights and provide links to exercise those rights.
- *Large Platform Providers.* The FTC will host a public workshop to better understand how Internet service

---

[4]Data enhancement occurs when a company combines data obtained from a third party with information it collects directly from consumers.

[5]The FTC declined to require affirmative, express consent for the collection of data about users between the ages of 13 and 17, but it stated that companies that target teens should consider additional protections, such as shorter retention periods for teens' data. The FTC also stated that social networking sites should consider implementing more privacy-protective default settings for teen users.

[6]The FTC believes that a "Do Not Track" system should: (1) be implemented universally to cover all parties that would track consumers; (2) be easy to find, easy to understand, and easy to use; (3) have choices that are persistent; (4) be comprehensive, effective, and enforceable; and (5) opt consumers out of the *collection* of behavioral data for all purposes other than those that would be consistent with the context of the interaction.

Continued on page 4...

FTC Releases Final Privacy Report . . .

Continued from page 3...

providers, operating systems, browsers, and social media companies track consumers' online activities comprehensively.

- *Enforceable Self-Regulatory Codes.* The FTC will participate in the Department of Commerce's project to facilitate the development of sector-specific, voluntary codes of conduct.[7] The FTC states that it will view adherence to strong codes of conduct favorably in connection with its law-enforcement work and will take action against companies that fail to abide by the self-regulatory programs they join.

Implications

The FTC's privacy framework is likely to have a significant impact on consumer data collection and use practices in all sectors of the economy. The final report is consistent with broader trends in this area, but it may particularly impact newer and emerging enterprises faced with limited resources for the kinds of efforts required to be consistent with the FTC's framework. The FTC made clear in its report that, to the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law-enforcement actions or regulations under laws currently enforced by it. However, it also is urging industries to adopt self-regulatory codes of conduct implementing the framework, and stated that it will take enforcement action against companies that fail to abide by the self-regulatory programs they join. Regardless of whether companies are bound formally by the framework, they should think carefully, and early on, about information governance strategy, especially where a business model depends upon or requires data monetization.

Wilson Sonsini Goodrich & Rosati's privacy and data security practice routinely advises clients on privacy and data security matters, including compliance with the FTC's consumer-protection initiatives. The firm also regularly assists companies with all legal aspects associated with the collection, use, and disclosure of consumer data. For more information on our privacy and data security practice, please visit http://www.wsgr.com/WSGR/Display.aspx?SectionName=practice/privacy.htm.

If you have questions on these topics, or on the report itself, please contact Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Tonia Klausner at tklausner@wsgr.com or (212) 497-7706; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; Matt Staples at mstaples@wsgr.com or (206) 883-2583; or Wendell Bartnick at wbartnick@wsgr.com or (202) 973-8963.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on March 29, 2012. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com

[7] For additional background on the Department of Commerce's privacy framework, including its efforts to facilitate the development of voluntary codes of conduct relating to consumer privacy, please see the WSGR Alert at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-consumer-privacy-bill-of-rights.htm. The FTC noted in its final report that staff from the FTC and the Department of Commerce sought to ensure that the agencies' privacy initiatives are complementary, and that the agencies will continue to work collaboratively to guide the implementation of their respective privacy initiatives.