WSGR ALERT

DECEMBER 2010

FTC RELEASES LATEST PRIVACY REPORT, PROPOSES NEW "DO NOT TRACK" MECHANISM

On December 1, 2010, the Federal Trade Commission (FTC) issued its latest report on privacy, *Protecting Consumer Privacy in an Era of Consumer Change: A Proposed Framework for Businesses and Policymakers.*[1] The report proposes a new framework for analyzing privacy issues, based upon three general principles: privacy by design, simplified choice, and greater transparency. The agency seeks public comment on the report, which has far-reaching implications for any business that collects, uses, or discloses consumer data.

In the wake of the report, businesses that collect, use, or disclose information about consumers either online or offline—regardless of whether that information is personally identifiable or not—may want to take a fresh look at their information practices. Businesses that depend upon collecting, using, and disclosing such information, especially those involved in online advertising, should consider providing comments to the FTC regarding the report and how the proposed framework may affect their business.

Scope of Proposed Framework

The agency has proposed a strikingly broad framework that builds upon its continued focus on consumer privacy issues over the past decade. The FTC proposal is intended to apply to all commercial entities that collect consumer data, both in online and offline contexts, whether or not they interact directly with consumers. Additionally, the FTC proposes that its framework extend beyond entities that collect "personally identifiable" information to include all commercial entities that collect data that reasonably can be linked to a specific consumer, computer, or other device. With this broad scope, the FTC continues to move away from a distinction between "personally identifiable" and "non-personally identifiable" information.[2] As a practical matter, businesses that have addressed data issues from the perspective that they do not collect personally identifiable information need to understand that this distinction is becoming increasingly less important.

Privacy by Design

The FTC proposes that privacy and security should be built into everyday business practices. Data should only be collected for legitimate business purposes, used only for those purposes, retained only as long as necessary to serve those purposes, and disposed of safely once no longer needed. In addition, businesses should implement procedures to ensure that the information they collect and retain is accurate.

The FTC also proposes that companies should maintain comprehensive data management procedures throughout their product or service lifecycles. This would entail procedures such as designating specific personnel responsible for privacy issues, conducting periodic reviews of privacy policies in light of relevant developments, and using privacy-enhancing technologies to establish and maintain strong privacy policies. The FTC advises companies to scale the size and scope of these programs to the risks presented to the data they collect, use, and maintain.

The proposal is consistent with broader trends in this area but may particularly impact newer and emerging enterprises faced with limited resources for these kinds of efforts. The report suggests that enterprises may want to think carefully, and earlier, about information governance strategy, especially where a business model depends upon or requires data monetization. If ultimately adopted, increased consumer control of data—and the need for accountability from and among data partners—seems highly likely.

Simplified Choice

When businesses are utilizing information beyond "commonly accepted" practices, the FTC also proposes that companies provide choices to consumers in a simpler, more streamlined way than in the past. Under this approach, when companies engage in certain commonly accepted practices such as order

[1] The full report is available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.

[2] In recent initiatives, the FTC has emphasized the decreasing importance of the distinction between personally identifiable and non-personally identifiable information, owing to changes in technology and an ability to re-identify consumers from purportedly "anonymous" data. *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf; Health Breach Notification Rule, 16 C.F.R. § 318 (2009) (requiring notice to an individual where an entity has a reasonable basis to believe data may be linked to that individual).

Continued on page 2...

FTC Releases Latest Privacy Report . . .

Continued from page 1...

fulfillment, internal operations, fraud prevention, and legal compliance—practices consumers have come to expect—companies would not need to provide notice and choice to the consumer. Notably, the FTC includes "first-party" marketing[3] as a commonly accepted practice that does not require consumer choice.

For most other practices, the FTC suggests notice and choice at the point of collection, in a way that is clear, concise, easy-to-use, and incorporates durable choice mechanisms. The FTC proposes that such choice be offered at a time and in a context in which a consumer is making a decision about his or her data. Furthermore, the FTC proposes that enhanced consent may be warranted in certain situations, such as when children, sensitive information, or deep packet inspection[4] are involved. While it is not clear from the report exactly what shape this enhanced consent will take, businesses should expect the agency to require some form of affirmative express consent, or even more heightened restrictions, when these situations arise.

The FTC suggests that consumers should be given better choices regarding the collection of information about them, not just the use of such information for direct marketing purposes. The FTC points favorably to a more uniform and comprehensive choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track," as a means for exercising choice in the context of behavioral advertising data collection. A Do Not Track mechanism would potentially function as a persistent Web browser setting that would inform websites of the consumer's privacy preferences. The importance of limitations on collection cannot be overstated. To the extent that the agency moves in a direction to encourage actively limiting data collection, the underpinnings of many established and emerging business models may come into question or require review for compliance.

The FTC notes several important considerations regarding any proposed Do Not Track mechanism. First, Do Not Track should be designed such that it does not undermine the benefits behavioral advertising has to offer, such as funding online content and providing more relevant ads that consumers value. Second, to avoid creating new privacy issues, Do Not Track should not require a registry of unique identifiers, as with the FTC's National Do Not Call Registry. Third, the FTC seeks comment on enabling more granular tracking control options that would allow consumers to select the types of ads they would like to receive and the types of data they are willing to have collected. Fourth, whatever form it takes, Do Not Track must be understandable and simple. Businesses that might be impacted by browser-level adoption of Do Not Track or other such proposals should consider reviewing the report carefully in light of their practices and participating in the proceeding through the submission of comments.

Greater Transparency

The FTC notes that privacy policies continue to play an important role in promoting transparency, accountability, and competition on privacy issues, but only promote transparency if they are clear, concise, and easy to read. In particular, the report critiques existing privacy disclosures for being both insufficient and too complex. As a solution, the FTC proposes that companies make privacy policies clearer, shorter, and more uniform so that consumers, regulators, and others may more easily compare policies among different companies. Given that many businesses may not have recently reviewed their privacy policies, or adopted such policies with a focus more directly upon personally identifiable information versus other information, a review and evaluation of the policy—and more importantly, the underlying practices—may be a prudent risk management strategy.

To further promote transparency, the FTC proposes that companies offer consumers access to the data they hold about them. 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. Recognizing the potential for burden in providing access, the FTC supports a sliding-scale approach to access under which the extent of access would depend on the sensitivity of data and its intended use. Broad consumer access to data collected and held by business may present particular challenges for smaller and newer businesses, and represents an area for careful study by many enterprises.

Finally, the FTC proposes that companies obtain affirmative opt-in consent from consumers before using consumer data in a materially different manner than claimed when the data was collected. For example, the FTC proposes that social networking sites obtain opt-in consent before making previously private information public. Additionally, the FTC asks for increased consumer education and awareness regarding commercial privacy practices. This particular proposal seems to reflect agency guidance and enforcement policy in the recent past and represents a more definite statement on this particular issue.

Implications

The proposed FTC framework is likely to have a significant impact on privacy practices in all sectors of the economy. In its report, the FTC criticizes industry efforts to self-regulate as too slow and as having failed to provide meaningful protection for consumers. Moreover, the FTC also takes issue with previous enforcement efforts that focused on harms to consumers. This may indicate a potential for increased enforcement in areas that enterprises have not focused on historically. In particular, the FTC claims in its report that its harms-based approach is limited

[3] "First-party" marketing is a company marketing to its existing customers and users. The FTC proposes that the concept only include the collection of data from a consumer with whom the company interacts directly for purposes of marketing to that consumer.

[4] "Deep packet inspection" generally refers to the ability of an Internet service provider (ISP) to inspect the contents of transmissions carried out over its network, including examining the contents of e-mail messages and Web sites visited.

Continued on page 3...

FTC Releases Latest Privacy Report . . .

Continued from page 2...

because, for some consumers, "the actual range of privacy-related harms is much wider [than physical or economic harm] and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'"

The report raises and seeks comment on several issues of significance to companies that collect, use, or maintain data about consumers. For example, the report seeks comment as to whether it is feasible for all companies collecting data that can be "reasonably linked" to a specific consumer, computer, or other device to be subject to the proposed framework. The report also indicates a potential for Do Not Track to be required by government mandate if it is not quickly adopted by industry voluntarily. Additionally, information brokers face a unique dilemma of determining how to effectively provide notice to consumers with whom they have no existing relationship. Finally, how will applying the core "fair information principle" of access to the general commercial context actually work in practice? The FTC seeks public comment on these matters through January 31, 2011. The complete list of issues upon which the FTC seeks comment can be found in Appendix A to the report, available at http://ftc.gov/os/2010/12/101201privacyreport.pdf#page=93.

Wilson Sonsini Goodrich & Rosati's privacy and data security practice includes more than 20 attorneys—including Lydia Parnes, the former director of the FTC's Bureau of Consumer Protection—who routinely advise clients on compliance with the FTC's consumer-protection initiatives, including its actions to prevent unfair and deceptive acts regarding the privacy and security of consumers' personal information. The firm also assists companies with all aspects of risk management associated with the collection, use, and disclosure of information.

If you have questions in these areas 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; Sara Harrington at sharrington@wsgr.com or (650) 493-4915; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; or Matt Staples at mstaples@wsgr.com or (206) 883-2583.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on December 13, 2010. 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