PATTON BOGGS LLP

March 28, 2012

FTC RELEASES FINAL PRIVACY REPORT AND FRAMEWORK FOR PROTECTING CONSUMER PRIVACY

Privacy and TechComm Client Alert

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Deborah Lodge
dlodge@pattonboggs.com

Paul Rubin
prubin@pattonboggs.com

Monica Desai
mdesai@pattonboggs.com

Mel Gates
mgates@pattonboggs.com

WWW.PATTONBOGGS.COM

On March 26, 2012, the FTC released its long-awaited privacy report and recommendations: "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (FTC Privacy Report). The FTC Privacy Report is available *here*.

The FTC Privacy Report details "best practices" for protecting the privacy of consumer data. Giving consumers greater control over the collection and use of their personal data is a key part of the best practices laid out in the FTC report. The FTC report warns that failure to implement and follow these best practices could expose companies to liability and FTC enforcement. The FTC also calls on Congress to enact general privacy legislation, data security and breach notification legislation, and data broker legislation.

The FTC Privacy Report propounds a privacy framework of fundamental principles for both companies and regulators to use in addressing consumer privacy issues. The FTC urges all companies handling consumer data to focus on the following fundamental principles in their privacy protection systems:

- **Privacy by Design:** Companies should build in consumer privacy protections at every stage in developing their systems and products, including providing reasonable security for consumer data, limiting collection and retention of consumer data, and adopting reasonable procedures to promote data accuracy.

- **Simplified Choice for Businesses and Consumers:** Companies should give consumers the option to decide what information is shared about them, and with whom. In the FTC's view, a consumer's affirmative consent should be obtained before data is used in a way that differs materially from what consumers consented to when the data was initially collected. The FTC also urges companies to adopt "Do-Not-Track" mechanisms to provide consumers with "a simple, easy way" to control the tracking of their online activities.

- **Greater Transparency:** Companies should disclose details about their collection and use of consumers' information, and provide consumers access to the data collected about them. Privacy notices should be clearer and more standardized to enable consumers to more easily understand and compare privacy notices and practices.

In the FTC Privacy Report, the agency indicates that it will focus its efforts on the following five areas during the next year:

Do-Not-Track - The FTC notes that commendable progress has been made in this area, including browser tools that allow consumers to limit data collection about them, the

Digital Advertising Alliance's icon-based system and compliance with the browser tools, and the World Wide Web Consortium's actions to develop "Do Not Track" standards for the online environment. The FTC commits to work with these groups to implement an easy-to-use, persistent, and effective Do Not Track system before 2013.

Mobile - The FTC urges companies offering mobile services to work toward improved privacy protections, including disclosures. To that end, the FTC will host a workshop on May 30, 2012 to address how mobile privacy disclosures can be short, effective, and accessible to consumers on small screens.

Data Brokers - The commission calls on data brokers to make their operations more transparent by creating a centralized website to identify themselves, and to disclose how they collect and use consumer data. In addition, the website should detail the choices that data brokers provide consumers about their own information.

Large Platform Providers - The report cites heightened privacy concerns about the extent to which various platforms and service providers, such as Internet Service Providers, operating systems, browsers and social media companies, seek to comprehensively track consumers' online activities. The FTC will host a public workshop in the second half of 2012 to explore issues related to comprehensive tracking.

Promoting Enforceable Self-Regulatory Codes - The FTC will work with the Department of Commerce and industry stakeholders to develop industry-specific codes of conduct relating to consumer privacy. The report states that the FTC will take compliance with strong self-regulatory privacy codes into account in its law enforcement efforts. If companies do not honor the codes they purport to embrace, those companies may face FTC enforcement actions.

The final FTC Privacy Report differs in a few key respects from the Interim Privacy Report issued by the FTC staff in December 2010. The final FTC Privacy Report concludes that the FTC privacy principles do not apply if a company collects only non-sensitive data from fewer than 5,000 consumers a year and does not transfer that data to third parties. In addition, the report concludes that data is not "reasonably linked" to an individual if a company takes reasonable steps to de-identify the data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it. Such "exemptions" will lighten the burdens of companies that anonymize data before transferring to third parties, or use limited personal data for only their own internal purposes.

In light of the FTC Privacy Report and its clear directives, companies that handle consumer data should review their policies and procedures and ensure that they comply with this new framework. We expect additional Congressional action in this area, as well as additional pronouncements from the Department of Commerce and other agencies – especially in light of the Consumer Privacy Bill of Rights issued by the White House on February 23, 2012.

The ultimate issue – what best practices should be followed in the consumer privacy area – has yet to be fully and finally determined. For example, the FTC Privacy Report calls for Congress to enact federal data breach notification legislation, and indeed various proposals are already pending in Congress. However, no bill has yet been passed by Congress.

Moreover, FTC Commissioner Rosch dissented from the FTC Final Report. Among his criticisms: 1) requiring a "Do Not Track" solution is premature as there are so many still-

unanswered technical and other questions; 2) “opt-in” solutions will necessarily become the de facto method for handling consumer data; 3) although characterized as only “best practices,” the Report's recommendations will likely be construed as federal requirements; and 4) the report contravenes the FTC's promises to Congress to avoid actions based on “unfairness” rather than “deception” grounds. These points are well-taken and deserve further discussion.

The final FTC Privacy Report is a must-read for virtually every company that collects or uses identifiable consumer data – online or otherwise. We expect additional developments in the consumer privacy area in the wake of this long-awaited FTC Privacy Report. Please contact us if you have any questions about the new FTC Privacy Report, the FTC’s recommended framework, and how they may apply to specific privacy practices and procedures.