December 6, 2010

FTC Wants Business to Change Its Overall Strategy Regarding Consumer Privacy; Proposes A "Do Not Track" Option Online

The FTC showed its hand this week, foreshadowing a crackdown on companies not adequately protecting consumer data, and proposing a "Do Not Track" list to protect consumers from behavioral advertising. In the wake of outlining an entirely new way of thinking of data protection for business, FTC Chairman Jon Leibowitz stated that the FTC "will take action against companies that cross the line with consumer data and violate consumers' privacy – especially when children and teens are involved."

On December 1, 2010, the FTC released a report entitled "Protecting Consumer Privacy in an Era of Rapid Change." In its report, the Commission proposes a framework for how companies that collect consumer data should protect consumers' privacy. The Commission also describes a series of roundtable meetings it will have to describe trends in data collection and consumer interests and their implications.

The proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be linked to a specific consumer, computer, or device. The proposed framework contains three components: (1) an emphasis on building data protection concepts and protections into their everyday business practices, branded by the FTC as "privacy by design"; (2) consumer notice and consumer choice within a company's data practices in a simpler, more streamlined manner; and (3) improved transparency of all data practices, including those of non-consumer facing businesses. The FTC report both explains the history of and proposes various protections to implement each of these three components.

The Commission urges companies to adopt a "privacy by design" approach, implementing and maintaining privacy protections as an integral part of each company's business practices. To effectuate the Commission's proposal, businesses should assign internal responsibility for securing consumer data and privacy oversight, train employees, and undertake privacy reviews of new products and services. Companies should also ensure that they obtain **only the data needed** for a specific business purpose and **safely dispose** of that data after it is no longer needed to fulfill that purpose. Businesses should ensure they collect and keep accurate data. The Commission acknowledges that the detail and energy devoted to privacy will vary by company, depending on the amount and nature of the data collected and how that data is used.

The Commission recommends that companies provide consumers with straightforward choices about how their data is collected and used. Businesses would generally be required to provide options to consumers in a manner both timely and contextually appropriate. Businesses would not be required to give consumer choices for commonly accepted practices, like fraud prevention and legal compliance. In the report, the Commission provides, as an example of an appropriate and relatively easily-implemented consumer choice mechanism, the "Do Not Track" option, which would require companies to include a setting, similar to a cookie, on a consumer's browser that would signal the consumer's choices about being tracked and receiving targeted ads.

Finally, the Commission proposes steps companies can take to ensure transparency of their privacy practices. The Commission suggests that companies should draft and enforce simple, understandable privacy policies; provide consumers with access to the data maintained about them; and implement notice and choice

practices, obtaining affirmative consent for all material, retroactive changes to their data policies. The staff also proposes that government and industry undertake efforts to educate consumers about their options with regard to how their data is collected, maintained and used.

This report has wide-ranging implications for any company that collects and maintains consumer data. If the FTC adopts its report, companies may be required to adopt new policies, create new positions, hire new personnel, and create consistent and user-friendly interfaces to keep in constant communication with consumers about how their data is used. Not only could compliance with these requirements prove costly and time-consuming to companies of various sizes, failure to comply could lead, in the future, to an increasing risk of FCC fines and other penalties.

Comments on the proposed framework and the protections contained therein must be received by the FTC by January 31, 2011.

If you have any questions, please contact Ted Claypoole, Jennifer Kashatus, Sarah Miller, or one of our other Womble Carlyle Privacy professionals.