MEMORANDUM: PRIVILEGED & CONFIDENTIAL

TO: ESPC Membership

FROM: D. Reed Freeman, Outside Counsel

DATE: March 29, 2012 FILE: 68223-1

RE: The Federal Trade Commission's Final Privacy Report

On March 26, 2012, the Federal Trade Commission (the "Commission") released its much anticipated final privacy report, *Protecting Consumer Privacy in an Era of Rapid Change*.[1] The report builds upon the preliminary privacy report released by the Commission in December 2010,[2] and it provides recommendations for businesses and policymakers with respect to online and offline privacy practices.

I. SUMMARY OF THE FINAL REPORT

The Commission's final report largely adopts the preliminary report. As in the preliminary report, it proposes a privacy framework that calls for companies to incorporate ***"privacy by design"*** into their practices, to offer consumers ***choice*** about how their data is collected and used, and to provide consumers with more ***transparency*** about their practices. The Commission, however, revises several elements and makes certain clarifications. The report presents the Commission's recommendations as "best practices" for companies that collect and use consumer data. ***Importantly, the Commission makes it clear that, to the extent that the best practices set forth in the report extend beyond existing legal requirements, they are not intended to serve as a template for law enforcement actions or regulation under laws currently enforced by the FTC.***

The Commission also takes the position in its final report that, because self-regulation has not yet gone far enough, flexible and technologically-neutral baseline privacy legislation is desirable. ***It intends the report to assist Congress in crafting such baseline privacy legislation.*** At the same time that it calls for legislation, the Commission encourages industry to continue and increase its self-regulatory efforts.

Finally, the final report sets out how the Commission has committed to promote implementation of the privacy framework over the next year. Specifically, it will focus its policy-making efforts in five main areas:

---

[1] The final report is available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[2] The preliminary report is available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

- **Do Not Track:** The Commission praises industry's progress in implementing an online Do Not Track mechanism, and it plans to work with industry to complete the implementation of an easy-to-use, persistent, and effective mechanism.

- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. Commission staff will host a public workshop on May 30, 2012, to address, among other issues, mobile privacy disclosures and how they can be short, effective, and accessible to consumers on small screens. According to the report, the Commission hopes that the workshop will lead to further industry self-regulation in this area.

- **Data brokers:** The Commission supports targeted legislation that would provide consumers with access to the information about them held by a data broker. The Commission also calls on data brokers that compile data for marketing purposes to further increase the transparency of their practices by considering the creation of a centralized website where data brokers could: (1) identify themselves to consumers and describe how they collect and use consumer data; and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

- **Large platform providers:** The Commission plans to host a public workshop during the second half of 2012 to explore the privacy issues associated with the comprehensive tracking of consumers' online activities by large platforms, such as ISPs, operating systems, browsers, and social media.

- **Enforceable self-regulatory codes:** The Commission will work with the Department of Commerce and industry stakeholders to create sector-specific codes of conduct. Commission staff will participate in that project.

II. THE PRIVACY FRAMEWORK

The Commission's privacy framework consists of the three principles of privacy by design, simplified consumer choice, and greater transparency.

A. The Scope of the Framework

The privacy framework applies to all commercial entities that collect or use online and/or offline consumer data that can be reasonably linked to a specific consumer or computer or other device.

There is an exception for entities that collect only non-sensitive data from fewer than 5,000 consumers per year and do not share the data with third parties, so as not to unduly burden small businesses.[3] The Commission did not, however, exempt from the framework's intended coverage those companies already covered by sector-specific privacy laws, such as

[3] "Sensitive data" includes Social Security numbers and financial, health, children's, and geolocation information.

the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. Instead, it emphasizes in the final report that the framework is intended to foster best practices but not impose conflicting legal obligations.[4]

The element of the framework's scope that generated the most comments was its application to "reasonably linkable" data. The Commission justified this application on the grounds that, not only is re-identification of supposedly "anonymous" data increasingly possible, but businesses have strong incentives to re-identify such data. Recognizing, however, that companies need certainty with respect to what constitutes "reasonably linkable" data, the Commission has taken the position that data is not "reasonably linkable" – and therefore not within the scope of the privacy framework – if the company possessing it implements the following protections: (1) reasonable measures to ensure that the data is de-identified; (2) a publicly commitment to using the data in a de-identified way; and (3) contractual prohibitions on downstream entities that use the data from de-identifying it, coupled with reasonable measures to ensure compliance with that prohibition.

B. The Framework's First Principle: Privacy by Design

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

This principle sets forth the best practice that businesses should treat consumer privacy systematically, both substantively and procedurally.

1. Substantive Principles

Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

The privacy framework calls for ***reasonable security*** for consumer data. The Commission notes that this obligation is already well settled, as it has a long history of enforcing data security obligations under Section 5 of the FTC Act and other laws. The Commission also commends efforts made by industry to ensure the security of consumers' data, but, nonetheless, ***it renews its call for Congress to enact comprehensive data security and breach notification legislation.***

The privacy framework calls for ***reasonable limits on data collection***. The Commission explains that reasonable limits are those that are consistent with the context of a particular transaction or the consumer's relationship with the business (or as required or specifically permitted by law). According to the Commission, a business should provide notice and choice for any inconsistent uses.

[4] The Commission urges Congress not to pass legislation that creates overlapping or contradictory requirements for entities subject to existing sector-specific privacy laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act.

The Commission states that companies should implement reasonable restrictions on the ***retention of consumer data*** and should dispose of it once the data has outlived the legitimate purpose for which it was collected. It also notes that retention periods can be flexible and scaled according to the type of relationship and the nature and use of the data. The Commission also calls on trade associations and self-regulatory groups to provide businesses with guidance about data retention and destruction policies.

According to the Commission, companies should maintain ***accurate data*** on consumers. As it does with other elements of the framework, the Commission believes that the best approach to achieving substantive accuracy is through a flexible approach, scaled to the intended use and sensitivity of the data at issue.

2. Procedural Protections

Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

The Commission explains that procedural protections are necessary to ensure that companies systematically consider consumer privacy throughout the design, development, and lifecycle of their products and services. It cites its recent settlement orders with Facebook and Google as containing the kind of comprehensive procedural protections it envisions: (1) designation of personnel responsible for the privacy program; (2) a risk assessment that covers, at a minimum, employee training, management, and product design and development; (3) implementation of controls designed to mitigate identified risks; (4) appropriate oversight; and (5) evaluation and adjustment of the program in light of regular testing and monitoring. The Commission also encourages the development and use of privacy-enhancing tools, such as encryption and anonymization.

C. The Framework's Second Principle: Simplified Consumer Choice

Companies should simplify consumer choice.

1. Practices Not Requiring Choice

Companies do not need to provide 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 or that are required or specifically authorized by law.

In an effort to simplify the choices given to consumers with respect to how their personal data is used and disclosed, the Commission proposed, in its preliminary privacy report, that choice should not be required for five commonly accepted practices: product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing. In its final report, the Commission, acknowledging that the list might be both over- and under-inclusive, and desiring to maintain a proper balance between consumer control and business flexibility, replaces it with a focus on the context of the interaction between consumer and business. Specifically, the privacy framework provides that companies do not have to provide 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 (or that are required or specifically authorized by law). While this standard relies to some degree on consumer expectations, it focuses on objective factors related to the consumer's relationship with the business. The five commonly accepted practices listed above are illustrative of the kinds of practices that do not typically require consumer choice.

In setting forth this standard, the Commission makes a few noteworthy comments regarding first-party marketing (which does not generally require consumer choice).

- First, companies that engage in ***extensive cross-site tracking for marketing purposes*** should provide consumers with choice with respect to such tracking, as the tracking would probably not be consistent with consumers' expectations regarding the services they receive from such companies. These companies may include, for example, ISPs and social networks that have plug-ins on third-party websites.

- Second, unless an affiliate or subsidiary relationship is clear to consumers (such as by common branding), such companies should be treated as third parties. This means, for example, that a company should not share its customer's data with an affiliate for ***the affiliate's own direct marketing purposes*** without first providing the consumer with choice with respect to that sharing.

- Third, companies should make efforts to increase the transparency of their ***data enhancement*** practices. The Commission does not suggest that companies obtain consent to such practices; however, it urges industry to rely on the other elements of the privacy framework to address the privacy concerns raised by it. In the Commission's view, this means that companies should, for example, explain to consumers how data enhancement works and how they can contact data enhancement sources directly. They should also encourage their data sources to increase their own transparency.

- Finally, the Commission notes that companies should generally obtain opt-in consent before collecting ***sensitive data*** for first-party marketing purposes, when its business model is specifically designed to target consumers based on such sensitive data. For example, Amazon would not have to obtain consent when recommending books about sensitive topics based on previous purchases of similar books, but a website collecting sensitive information to target ads to consumers based on particular medical conditions would.

2. Practices Requiring Choice

For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

The Commission explains that data use and disclosure practices that are inconsistent with the context of the transaction or the company's relationship with the consumer (or that are

required or specifically authorized by law) require consumer choice. Although the Commission has supported the use of "just-in-time" privacy notices and choice mechanisms, it does not impose any one-size-fits-all method of complying with this best practice, noting, in fact, that there are contexts (particularly offline) where it may be appropriate to give consumers choice after the transaction where data was collected. The Commission recognizes that precisely how companies achieve the goal of providing meaningful choice will vary across industries, and it notes that industry is well-positioned to design and develop the choice mechanisms that are most appropriate for it.

The Commission also addresses choice in a few particular contexts:

- **Take It or Leave It Choice:** The Commission addresses the scenario of a "take-it-or-leave-it" choice, whereby a consumer must agree to a particular use or disclosure of his or her personal data in order to receive a product or service. It explains that such a scenario may raise privacy concerns, especially if there is inadequate competition in the market for the product or service (such that the consumer does not have viable options), the product or service is essential, and/or the terms of the choice are not clearly and conspicuously disclosed.

- **Do Not Track:** The Commission has consistently advocated for choice with respect to online behavioral advertising and, while its report commends industry for the steps it has taken to date, it also renews its call for implementation of a universal Do Not Track system. In its view, such a system should: (1) be universal; (2) be easy to find, understand, and use; (3) be persistent, with choices that do not revert or get overwritten; (4) be comprehensive, effective, and enforceable; and (5) opt consumers out of behavioral data collection for all purposes (not merely marketing), other than those which are consistent with the context of the consumer's interaction with the company doing the tracking. The Commission does not call for Do Not Track legislation in this report.

- **Large Platform Providers:** The Commission explains that, even if a company has a relationship with a large platform provider – such as an ISP, operating system, browser, or certain social media sites that collect data across the Internet – its tracking of the consumer may be inconsistent with its relationship with him or her and therefore warrant choice. As noted above, the Commission plans to convene a public workshop during the second half of 2012 to address privacy issues associated with large platform providers' collection of consumer data.

- **Affirmative Consent for Certain Practices:** The Commission identifies two practices that it believes require affirmative express consent. ***First, companies should obtain affirmative express consent before making material retroactive changes to privacy representations.*** This position is not new; the Commission has expressed it repeatedly for at least eight years, and it has imposed it in settlement orders in more than one enforcement action. ***Second, companies should obtain affirmative express consent before collecting sensitive data,*** such as information about children, health and financial information, geolocation data, and Social

Security numbers. In addition, social networks and others specifically targeting teens should take extra precautions with respect to their submission of personal information.

D. The Framework's Third Principle: Greater Transparency

Companies should increase the transparency of their data practices.

The Commission's formulation of its transparency principle is unchanged from its preliminary report. The principles focuses on providing consumers with better awareness of how and for what purposes companies collect, use, and share data, through privacy notices, access to data, and consumer education.

1. Privacy Notices

Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.

The Commission calls for the simplification of privacy notices, such as through the use of standardized terminology, format, and/or other elements. In the Commission's view, members of various industry sectors should work together to create standards relevant to their industry, possibly through the multistakeholder process that the Department of Commerce plans to convene.

According to the Commission, the need for simplification and industry involvement is particularly acute in the mobile realm, given the number of entities that want to collect user data and the limited space for disclosures. As noted above, the Commission plans to address mobile disclosures in a May 30, 2012 public workshop.

2. Access

Companies should provide reasonable access to the consumer data they maintain. The extent of access should be proportionate to the sensitivity of the data and the nature of its use.

According to the Commission, consumers' access to the data that companies hold about them should be proportional to the sensitivity and intended use of such data. With respect to sensitivity, it addresses three types of data that are relevant:

- **Marketing data.** The Commission urges businesses that maintain data for marketing purposes to provide consumers with access to such data and permit them to suppress categories they would not like used for targeting. The Commission does not propose more individualized access and correction rights, but it encourages companies to provide them, if feasible.

- **Data subject to the Fair Credit Reporting Act (the "FCRA").** Companies that collect and provide data that others use to make employment, credit, or insurance

eligibility decisions are subject to the FCRA and its stringent data privacy, use, and access requirements. In its final report, the Commission discusses recent enforcement actions that demonstrate the FCRA's broad reach.

- **Other types of data.** With respect to businesses that maintain other types of data, the Commission supports a system where consumers' access to their data is scaled to the data's uses and sensitivity. At a minimum, consumers should be able to access the kinds of information collected and the sources of that information. If sensitive data is collected or data is used in unexpected ways, more specific access may be required. According to the Commission, reasonableness is the touchstone.

The Commission makes further recommendations with respect to two specific contexts. First, as noted above, it supports legislation that would require ***data brokers*** to give consumers access to the data they hold about them. It also recommends that data brokers coordinate to create a centralized website that describes the kinds of data they collect and to whom they sell it. Second, the Commission expresses general support for the idea of ***an "eraser" button*** that would allow individuals, and especially teenagers, to delete data previously posted online. The Commission recognizes, however, that such a tool raises a variety of potential legal and technical issues, including First Amendment issues.

3. Consumer Education

All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

The Commission encourages companies to continue to engage in consumer education efforts and invites industry to re-brand and use the Commission's own materials.