



Comments on the Preliminary FTC Staff Report on Consumer Privacy

Christopher Wilson
Director and Counsel, E-Commerce & Telecommunications
February 18, 2011

TechAmerica is pleased to respond to the Federal Trade Commission's ("FTC" or "Commission") *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* ("Staff Report").¹ TechAmerica's members have a vested interest in the success and future of the Internet and TechAmerica welcomes the opportunity to file comments on behalf of its members in this proceeding.

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,200 member companies of all sizes from both the public and commercial sectors, TechAmerica is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association ("AeA"), the Cyber Security Industry Alliance ("CSIA"), the Information Technology Association of America ("ITAA") and the Government Electronics and Information Association ("GEIA").

Representing all sectors of the information technology industry, TechAmerica has a broad and diverse membership. TechAmerica's members include, for example: (a) manufacturers and suppliers of broadband networks and equipment; (b) consumer electronics companies; (c) information and communications technology hardware companies; (d) software and application providers; (e) systems integrators; (f) Internet and e-commerce companies; (g) Internet service providers; (h) information technology government contractors; (i) information technology consulting and sourcing companies; and (j) information technology security companies.

¹ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) ("Staff Report").

Introduction

TechAmerica appreciates the FTC's efforts to review consumer privacy in an "era of rapid change." Consumer privacy has been and remains a core focal point for a large number of participants in the Internet industry, regardless of whether or not they interact with consumers directly.

TechAmerica generally supports the Commission's three core principles: 1) Privacy by Design; 2) Simplified Choice; and 3) Greater Transparency. However, TechAmerica believes that self-regulation and industry codes of conduct should remain at the forefront of any consumer privacy reform efforts. TechAmerica respectfully disagrees with the Commission's conclusion espoused in its Staff Report that "...industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."² The relatively young Internet industry has developed self-regulatory initiatives that respond pro-actively and quickly to the rapidly evolving technology environment. Innovative solutions implemented by advertising networks, web browser companies, and consumer-facing websites, for example, have provided consumers with more choice and control over the collection and use of their personal information.³

Privacy by Design

TechAmerica appreciates the Staff Report's acknowledgement of the efficacy of "privacy-enhancing technologies" to protect consumer privacy.⁴ TechAmerica has previously stated publicly its support for the concept of "privacy by design,"⁵ and wholeheartedly believes that technology is much more likely to enable the protection of consumer privacy rather than risk violating it. Whether these

² *Id.* at iii.

³ Examples include the guidelines and standards of the Direct Marketing Association ("DMA"), Interactive Advertising Bureau ("IAB"), the Network Advertising Initiative ("NAI"), TRUSTe, the AICPA's WebTrust, and BBBOnline, as well as Google's "Keep My Opt-Outs" browser extension and Microsoft's "Tracking Protection" browser functionality.

⁴ Staff Report at 52.

⁵ See TechAmerica Comments to the Department of Commerce's Internet Policy Task Force, at 4, *available at* <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/TechAmerica%20Comments.pdf> (June 14, 2010).

privacy-enabling technologies are software-based, hardware-based, integrated into a network, or accessed via a website, these technologies will facilitate consumer trust and ensure that both offline and online commerce continues to grow.

TechAmerica believes that all companies, to the extent possible, should implement “privacy by design” concepts within their organization’s business model. “Privacy by design” is a concept that should be part of an accountable company’s overall approach to supporting privacy in an environment of technological change and information-intensive innovation. To achieve its objective, the “privacy by design” principle should avoid detailed “one size fits all” standards. A rigid “privacy by design” standard would decrease the time an entity has to market its products and services and increase production costs, and thus increase final product costs to consumers. Instead, a “privacy by design” accountability model should focus on encouraging privacy as a foundational part of organizations’ people and business processes. Core concepts applicable before, during, and after the developmental process, such as data security, reasonable data collection limits, sound retention practices, and data accuracy can all be included as a “privacy by design” framework as implemented in self-regulatory frameworks.

TechAmerica does not believe that “privacy by design” should be mandated via a prescriptive government-imposed policy regime. Companies are in the best position to determine how to implement “privacy by design.” Indeed, many of TechAmerica’s member companies already implement some aspects of “privacy by design” in their organizations’ business models.

It is imperative that companies have the flexibility necessary to implement “privacy by design” principles internally to best match their business models and their interactions with customers. For example, the FTC should refrain from prescribing a rigid “privacy by design” framework, especially to the extent that such a framework includes elements such as requiring a “reasonable retention period” for data or defining what constitutes a “specific business purpose” for data collection. Most organizations retain data based on the context or types of documents and environments in which it is used. The

notion that a particular data element can or should be deleted at the same time regardless of its many forms is not accurate. There are a variety of business and legal obligations that impact each organization's retention needs, and a government imposed mandate is not feasible or prudent. Even in the European Union, where some of the most challenging privacy mandates are in place, it is business need and not arbitrary government timelines that determine retention periods.

Simplified Consumer Choice

TechAmerica supports the FTC's general statement that a more "simplified approach to offering and communicating privacy choices" is needed.⁶ Consumers, especially those participating in the online marketplace, should be provided with a meaningful and appropriate opportunity to exercise choice for certain uses of personally identifiable information.

TechAmerica appreciates the FTC's recognition that certain "commonly accepted practices" do not require consumer consent, especially those involving fraud prevention and first party marketing. However, TechAmerica cautions against the Commission adopting a detailed definition of what constitutes such "commonly accepted practices." Nonetheless, any list of "commonly accepted practices" should include, at a minimum, network security, identity verification,⁷ and commonly-branded affiliate first-party marketing because consumers would expect that their personal information would be used for all such purposes. However, the Staff Report fails to take these necessary practices into consideration. Indeed, requiring choice for network security and identity verification would be counter-intuitive, as cyber criminals would most assuredly not consent to the use of their personal information. Faced daily with changing technologies and consumer demands, the technology industry is best positioned to determine the scope of such "practices."

⁶ Staff Report at 52-53.

⁷ This is especially applicable to public record data accumulated and shared from third party providers for vetting purposes.

Moreover, TechAmerica does not believe that a one-size-fits-all method of providing meaningful choice is prudent or needed. Companies, especially technology companies, must have the flexibility to meet consumer expectations and technological advancements in this “era of rapid change.” This is evidenced by the development of technological tools that provide consumers more control over how their personal information is used for advertising purposes, for example. In this vein, the Staff Report discusses the efficacy of a “Do Not Track” mechanism in order to give consumers more choice.”⁸ Within the last few months, at least three major web browsers have implemented a technological tool that enables consumers to prevent online tracking of their activities.⁹ Indeed, companies are competing to provide consumers with this capability absent a government mandate to do so.¹⁰ Notwithstanding these developments, there are a number of technical obstacles in place that have not been addressed in the report or resolved in practice. Thus, any legislative or regulatory mandate in this regard is unnecessary and potentially detrimental to the current industry initiatives to provide consumers with the proper technological tools to effectuate their choices.

Greater Transparency

TechAmerica agrees with the Commission’s Staff Report that the creation of simplified privacy policies written in plain English are certainly welcome. In order to facilitate consumer awareness and understanding, industry should promote transparency in their practices and procedures used to collect, store and use consumer information.¹¹

However, members of the technology industry must be allowed to develop industry self-regulatory standards regarding when and how notice and choice mechanisms are posted. As the Staff

⁸ Staff Report at 63-64.

⁹ These are Google’s “Keep My Opt-Outs” browser extension for Chrome, Microsoft’s “Tracking Protection” feature on IE9, and Mozilla’s use of a “Do Not Track HTTP” header for Firefox.

¹⁰ See, e.g. www.anonymizerinc.com.

¹¹ For example, for some companies, it may be feasible to implement a standardized color and number-coded icon system, which could be usable both offline and online. The system would provide consumers with an easy-to-understand manner to determine how and to whom their personal information is used and shared.

Report recognizes, changes in technology and user interfaces present challenges with respect to how consumers are informed about privacy practices (e.g., small mobile screens).¹² Because of these challenges, transparency cannot equate to a prescriptive format that does not allow each sector, and each organization, to advise its customers of its full privacy practices in the form and manner it deems appropriate.

TechAmerica agrees with the Staff Report that further consumer education regarding commercial data privacy practices is needed. Considering e-commerce is in its “adolescence” (15 years old) and social networking is in its “early childhood” (less than 10 years old), consumers are still learning about the dynamic nature of the Internet and the use of consumer information, especially in comparison to the offline world. Comprehensive consumer education requires a multi-stakeholder approach. But the technology industry, whether via individual companies or industry associations, has already taken significant steps towards improving consumer awareness. These efforts must continue. And they will.

Conclusion

TechAmerica appreciates the opportunity to present its views on the important issue of protecting consumer privacy. Representing all segments of the technology industry, TechAmerica fully recognizes the importance of consumer trust and technological innovation. Indeed, both go hand-in-hand. As the Commission continues to evaluate its proposed framework, TechAmerica looks forward to providing constructive input in order to achieve a framework that protects consumers and encourages, rather than stifles, innovation.

¹² Staff Report at 72.