Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

Comments of the

Software & Information Industry Association

on the

Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers

February 18, 2011

The Software and Information Industry (SIIA) appreciates the opportunity to comment on Federal Trade Commission's (FTC) *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Report). The Report is thorough, thoughtful and timely, and it provides many positive recommendations for updating existing concepts of privacy protection in order to respond to the challenges of new technology and business practices.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education and consumers.[1] SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

For over a decade, SIIA has worked with policymakers at the Federal and state levels in the United States, and also with policymakers in Europe, Canada and other regions, to examine the implications and operations of privacy and related laws. This has included work with the relevant Federal agencies implementing existing privacy and security regulations and policies, notably, the Federal Trade Commission's (FTC) approach on

---

[1] Our website can be found at: www.siia.net

unfair and deceptive trade practices, as well as implementation of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Health IT Act. SIIA has also forged productive working relationships with state policymakers on the myriad state privacy and data security laws and initiatives, as well as with foreign governments, notably Canada and the European Union (EU).

General Comments

As we recently noted in our comments to the Department of Commerce's (DOC) "Green Paper" on Privacy,[2] SIIA appreciates the administration's careful consideration of this important issue at this time. SIIA strongly supports the balance between privacy and the free flow of information, as well as the balance between the need for consumer confidence and continued innovation. To that end, we appreciate the FTC, the DOC and the Administration for taking such a thorough, thoughtful approach, rather than rushing to make policy recommendations at this time. In an era of rapidly changing technology and business models, the development of a fixed regulatory framework for privacy protection is a counterproductive exercise. Therefore, SIIA strongly cautions against the implementation of unnecessary legislation or regulations, in favor of a framework that is industry-led, voluntary and enforceable.

The FTC's proposed privacy framework calls for companies that collect or use consumer data to adopt certain privacy protections to ensure that consumers and other data subjects are protected from privacy-related harm. The Report combines elements of the previous policy frameworks used by the Commission – the notice and consent and the harm frameworks – to craft a checklist of good information management practices that companies can use as they design the systems and business practices or update them to provide new products or services to their customers. The key elements of this new privacy framework include:

- Data security, reasonable collection limitations, sound retention policies and data accuracy;
- Choice on the collection and use of data at the time of data collection, except for certain commonly accepted business practices;
- Clearer, shorter and more standardized privacy notices;
- Special choice for online behavioral advertising: Do Not Track; and
- Reasonable access to data.

[2] http://siia.net/index.php?option=com_docman&task=doc_download&gid=2796

SIIA supports the principle endorsed in the report that certain "commonly accepted business practices" involving the collection and use of information do not require consent.

One of the major difficulties in the notice and consent framework is that a practice of universal consent is unnecessary and unworkable for many companies and consumers. For that reason, many privacy statutes create exceptions for certain normal business activities, where consent is neither practical nor required. The Fair Credit Reporting Act (FCRA) and the privacy provisions of the Gramm Leach Bliley Act (GLBA) contain such exceptions on consent. In some cases, these exceptions are needed to allow important commercial and economic activities to take place, including many activities and uses for data that redound to the clear benefit of consumers. In other cases, the activities may be so routine or expected that tacit consent can be assumed, and obtaining consent would simply be intrusive and burdensome for all parties.

SIIA supports the general principle of "Privacy by Design.

The concept of "Privacy by Design" is a very good one, as suggested in the Report. It is indeed a useful tool for businesses to evaluate corporate privacy and data security practices to identify potential vulnerabilities (p. 44-52). It is often less expensive and more effective to design systems to provide for privacy than it is to try to retrofit systems to advance this objective after the fact. Policymakers in certain jurisdictions have already recognized that. For example, the privacy commissioner in Ontario has been leading efforts to persuade companies to think strategically about providing privacy protections from the ground up. SIIA believes that companies adopting this approach can better serve their customers, and SIIA supports the FTC's general recommendation on this issue. However, we believe that such an approach should remain voluntary so as to avoid undercutting the practices that best suit their respective customers, without stifling innovative approaches.

SIIA agrees with the suggestions in the report that privacy protections depend on the context of information collection and use.

One of the concerns about standardized information practices is that the way in which a legitimate principle should be applied often depends on the context of information collection and use. As privacy scholars such as Helen Nissenbaum have argued persuasively, an essential aspect of privacy is the right to an appropriate flow of information. According to her , the appropriate flow of information is defined by context-

dependent information norms.[3] For instance, the socially entrenched norms governing the flow of information in a medical context differ from the informational norms in a financial context, and both are different from the flows expected in the context of relationships among friends. Therefore, privacy policy frameworks should respect the context-dependent nature of privacy norms. In many places in the Report, the FTC staff acknowledges that privacy protections depend on the context of information use.

SIIA believes that the framework should be a checklist for companies, not a regulatory standard.

The FTC suggests that the framework may serve as a guide for policymakers, including the U.S. Congress, as they "develop solutions, policies, and potential laws governing privacy" (p. i). It also suggests that the purpose of the framework is to "guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines." (p. i). Finally, it describes the Report as proposing a "normative framework for how companies should protect consumers' privacy." (p. i)

SIIA believes that the FTC framework should be a checklist for companies. It should be a guide for them to consider as they develop their information management practices. It should *not* be used as a standard for industry-wide self-regulatory activities, since its application will depend crucially on the context and business models involved . It should *not* be used as the basis for legislation or for government regulations, and it should *not* be construed as setting standards that the FTC will use to determine unfair or deceptive acts or practices. The framework provides an excellent review of information practices that companies should take into account as they build their information management practices. However, as described below, at key points the framework lacks the clarity and precision that would enable an outside entity to determine whether a company is or is not in compliance with it. Despite the efforts of the FTC staff, providing the necessary clarity and consistency may not be feasible in an area where innovation and technological advancements are so rapid.

[3] Helen Nissenbaum Privacy in Context Stanford University Press, 2010

The FTC should provide additional guidance by defining the harms that companies should try to prevent in their collection and use of information.

The FTC wants to incorporate elements of the harm framework in its new approach, but is concerned that the harm framework construes "harm" too narrowly. It then falls back on the idea that the harm involved in failing to follow privacy rules is the failure to follow the rules. In this way, lack of consent, instead of leading to harm becomes the harm (p. 20). However, as legal scholars such as Paul Ohm[4] and Daniel Solove[5] have pointed out, the purpose of privacy rules is to prevent harms before they happen. Many scholars also suggest that the important thing is to regulate the harmful uses of information, and to put less emphasis on regulating the collection or analysis of information.[6] While harms can be limited to tangible damages such as physical damages and economic losses, there is no need to limit the concept in this way—leading proponents of the harm concept do not do so. [7]The key question becomes how to identify these harms. The FTC could aid companies in developing their information management practices by defining the harms that companies should seek to avoid in their collection and use of information. Therefore, SIIA recommends that the FTC provide better definitions of "harm" or at least articulate several examples or categories of what constitutes "harm."

Scope

The FTC report applies its framework to commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer. It is intended to apply to both online and offline contexts and to all companies regardless of whether they interact directly with consumers (p. 42). The FTC should clarify three interrelated scope issues.

---

[4] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review ____ (forthcoming 2010) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[5] Daniel Solove, "A Taxonomy of Privacy," in Understanding Privacy, Harvard University Press, 2008.

[6] See Daniel Solove, The Digital Person, New York University Press, 2004, pp. 91-92 and T.Z. Zarsky, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society," 56 Maine Law Review 13 (2004), p. 15.

[7] J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information 75 U. Chi. L. Rev. 109 2008 ("Beales and Muris"), pp. 116-117. See also remarks of Howard Beales, p. 10 Exploring Privacy: An FTC Roundtable Discussion December 7, 2009, Panel 5 Exploring Existing Regulatory Frameworks at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess5.pdf

1. The FTC should provide clear guidance as to what counts as "reasonable" linkage in determining which information is covered by the guidelines.

The FTC notes that the distinction between personally identifiable information and other information has been harder to maintain as analytic techniques and ubiquitous data collection have made it possible to use virtually any piece of information about a person to identify him or her with a surprising degree of accuracy. Paul Ohm has noted this phenomenon and its implications for privacy policy. Potentially all information is linkable with sufficient resources and analytic techniques, with the result that all information pertaining to a person is subject to the privacy rules.

The FTC attempts to respond to this situation by the use of the concept "reasonable" linkage. It recognizes that its notion is not well defined and asks for further comment in resolving questions associated with it. SIIA urges the FTC to provide further limiting specifications on the concept of reasonable linkage so as to guide business seeking to manage their information systems appropriately.

2. The FTC should clarify which parts, if any, of the privacy framework apply to companies that obtain and use covered information but have no connection with the data subjects, and to companies involved solely in business to business transactions.

Many companies do not obtain data directly from the data subject but obtain it from entities that collect it from the public. Many of the transactions involving information about individuals take place solely between businesses or sometimes even between businesses and government entities. In these circumstances, some of the elements of the framework do not apply, and there is a question whether any of it should apply. For example, obtaining consent to use the data would not be feasible. A requirement that these companies get permission from each data subject for all further uses of this information would block many important uses of information. There is a strong case that further use of government public record data, public directories and published news reports, which are already in the public domain, should generally be beyond the scope of the framework. As the FTC builds out its framework, it would be helpful for companies to know the extent to which the FTC intends the framework to apply to these cases.

3. The FTC should specify which offline information collection and use practices it wishes to cover.

The FTC Report suggests that the framework should apply broadly to both online and offline activities. In many ways, online activities have a similarity of electronic form and content and the measures taken to comply will have a certain commonality. However, the offline world contains thousands of contexts and variations in information collection and use. It is not clear whether the FTC means to include all this variety of offline contexts and variations. Some contexts are already regulated under other statutes. This includes financial services and health information. Other industries such as telecommunications are not directly under the FTC's jurisdiction. The FTC should clarify whether these industries are excluded, and whether all other industries and contexts are covered. Otherwise the lack of specificity regarding which practices are covered will make it hard for enterprises to know when the framework applies and when it does not.

Simplified Choice

The Report seems to recommend a practice of universal notice and choice regarding the collection and use of data at the time of data collection, except for certain commonly accepted business practices. SIIA believes this policy recommendation needs further analysis and that there is an alternative approach that might more effectively accomplish its goals.

It is worth noting that the most comprehensive and detailed notice regime is that which applies to the financial services industry, and it is widely regarded as an expensive failure. Billions of dollars have been spent on notices that virtually no one reads and would not communicate in a meaningful way if read.[8] The FTC report responds to this by calling for simplified choice. However, the problems might be more fundamental than the complexity of the notices.

In addition, choice structures and mechanisms should be arranged to prevent privacy harms. The FTC's Do Not Call regulation was designed to give consumers the ability to opt out of receiving intrusive unsolicited telemarketing calls. There was a widespread recognition of the harm involved in this practice – unwanted and disruptive intrusion into

[8] Fred H. Cate, The Failure of Fair Information Practice Principles, in Consumer Protection In The Age Of The Information Economy (Jane K. Winn ed., 2006) ("Failure of Fair Information Practice Principles") http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972 (noting at p. 365 that financial privacy notices cost an estimated $2-5 billion)

the home. The regulation is enormously popular, with more than 200 million telephones registered on the Do Not Call list. The predictable result of this regulation was a dramatic reduction in the number of unsolicited calls. Importantly, when the regulation was under consideration, this highly-predictable outcome was critical to generating sufficient support for the regulation. The predictable result was understood and even welcomed as a desirable outcome of the regulation. On the contrary, the proposed framework does not provide an assessment of the likely outcome for a universal regime of simplified notice and choice. This concern is especially worrisome in the case of the Do Not Track proposal discussed below.

SIIA recommends that in considering a model for the use of notice and choice in the privacy area, the methodology should be to first identify the harm to be prevented, and then arrange individual choice to reach that goal. Predictable outcomes should be evaluated in advance. Instead the FTC seems to recommend easy, convenient choice in all circumstances except for those on a specific list without a careful analysis of the predictable results of this recommendation.

Choice structures often produce predictable results. For example, in the days of the monopoly telephone industry, the telephone company provided privacy for those who did not want their telephone numbers to be publicly known by allowing them to request an unlisted number. The default was that the number would be listed, but a mechanism was provided for those who wanted privacy. If the default had been reversed, it is unlikely that many people would have contacted the telephone company to ask that their number be listed. The result would have been that telephone directories would have been too expensive and too thinly populated to be produced. Telephone companies chose an opt out choice mechanism to avoid this predictable result.

A hypothetical example also illustrates how a choice structure can produce predictable results. A requirement that television sets be designed to allow easy and convenient suppression of commercials would almost certainly lead audiences to skip the commercials and concentrate on the programs. However, over time, the lack of an audience for advertising would dry up that funding mechanism for television programming, and viewers would need to pay higher subscription fees. Free, over the air television would no longer be economically sustainable. Therefore, a proposal to provide easy suppression of commercial material on television needs to be evaluated in light of this predictable result, and imposed only if that outcome is an intended or at least acceptable goal of public policy.

Cass Sunstein and others have noted the importance of arranging choice structures so as to accomplish the goals that participants in the marketplace would have wanted for themselves.[9] SIIA urges the FTC to undertake this type of analysis before recommending universal notice and choice. It should identify the specific privacy harms that a notice and choice mechanism is designed to avoid. It should also recommend that institutions that collect and use consumer information provide appropriate notice and choice only in those circumstances.

Commonly accepted business practices

If the FTC adopts a recommendation of universal notice and choice with exceptions, SIIA thinks it should adopt several modifications. SIIA agrees that the business practices listed by the FTC should not trigger an obligation to provide notices, including product fulfillment, internal operations, fraud prevention, legal compliance, public purpose, and first-party marketing.

In addition, the FTC should add other business practices to the list. Some of these practices provide social benefits that should be preserved such as the location of witnesses or the monitoring of registered sex offenders. Others are familiar and widely accepted practices such as the use of business cards collected at exhibitions for follow up contact from a vendor.

The need to confirm that such business practices do not trigger a notice obligation illustrates the weakness of the approach of universal notice with exceptions. A more workable approach, as indicated above, would be a list of circumstances under which notice and choice would be required.

The FTC's inherently conservative approach of excepting only commonly accepted business practices creates a problem of what to do about new business practices. The only practices that could qualify under the exception would be existing practices. New practices would not commonly be excepted simply because they are new. However, many new innovative practices would have large social benefits if they were allowed to find their place in the marketplace or in the common practice of public institutions. The FTC should not prevent or restrict the development of these new and beneficial uses of information by imposing a notice and consent requirement on them for the sole reason that they are new.

---

[9] Richard Thaler and Cass Sunstein, Nudge, Penguin Books, 2009

SIIA suggests that the FTC address this issue of new business practices by leaving their status to the reasonable judgment of the marketplace actors involved. This will allow new practices to get a foothold in the market. The FTC can recommend that they be subject to a notice and choice regime if experience with the practice suggests that notice and choice would have good results.

Do Not Track

The FTC proposes to allow consumers to choose whether to allow the collection and use of data regarding their online searching and browsing activities, typically through the use of persistent cookies which would signal their choices to various Internet actors. SIIA thinks that a regulatory requirement to this effect might have harmful effects. A recent study estimated that targeted ads generated almost three times the revenue of regular run of network ads and accounted for 18% of the total website ad revenue.[10] As many website publishers themselves have noted, restrictions on advertising through ad blocking would risk undermining their economic basis. [11] A mandated Do Not Track regime might have a similar result.

SIIA notes that the FTC report adopts the principle that a do not track mechanism should not undermine the benefits of online behavioral advertising. SIIA recommends that the FTC take steps to ensure that its own recommendation preserves the benefits of online behavioral advertising and urges it to monitor the marketplace to ensure that any private mechanisms are effective in promoting consumer choice and preserving the benefits of online behavioral advertising.

SIIA believes that Industry is developing sufficient mechanisms to provide the appropriate level of choice to consumers. To that end, a coalition of businesses and industry groups recently launched the Self-Regulatory Program for Online Behavioral Advertising in October 2010.[12] It is critical that the FTC recognize that such industry efforts have made

---

[10] Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, March 24, 2010 available at http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf. The study was done by Howard Beales, former director of the FTC's Bureau of Consumer Protection.

[11] See Ken Fischer, Why Ad Blocking is Devastating the Sites You Love, ArsTechnica, March 6, 2010 at http://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars

[12] For example, the industry has developed an advertising option icon lets consumers know when an advertisement is based on behavioral information. See www.aboutads.info/choices.

tremendous progress in developing mechanisms to provide the appropriate level of choice to consumers. SIIA is confident that the industry-developed choice mechanism will sufficiently balance the needs of consumers and advertisers and content sites.

For instance, movement within a company's own website or suite of products is clearly not the kind of tracking that consumers are concerned about, and it is vital for businesses to track this kind of movement in order to optimize the performance and appeal of their websites. Similarly, websites routinely log the identity of the websites from which visitors arrive and to which they go when they leave. This provides valuable information about what attracts visitors to the site and what provides them with an incentive to leave. In an industry-led choice regime, these tracking activities would be permitted.

The FTC suggests the use of the browser mechanism to implement a do not track requirement. However, less and less Internet activity is conducted through the browser and more is done through applications such as instant messaging, voice over internet, RSS feeds, and streaming video. These applications use the Internet's underlying communications protocols, but they do not use the browser capabilities.[13] Therefore, a browser-based do not track mechanism would be insufficient. An industry-led initiative would be best suited to handle technological innovations and developments of this nature.

Finally, tracking information has numerous potential uses other than targeted online behavioral advertising. Outside of any advertising context, many software and information companies use consumer data to deliver personalized services and to deliver content to users based on information they know about the user, such as improving search and better tailoring applications and offerings to customers based on their preferences. It is often used for fraud prevention, risk management, control of spam and malware, intrusion prevention or detection. Government-mandated anti-tracking mechanisms might short circuit the development of these valuable uses of tracking information. On the contrary, an industry-led do not track initiative would likely be more able to accommodate valuable uses while still allowing appropriate user control.

---

[13] Chris Anderson and Michael Wolff, "The Web is Dead. Long Live the Internet," Wired, August 17, 2010 http://www.wired.com/magazine/2010/08/ff_webrip/all/1

Clear, concise, and easy to read notices

The FTC staff report is correct in pointing out the limitations of the existing notice regime for Internet privacy. Notices are virtually unread and the economic cost if they were read would be enormous. In 2009, researchers at Carnegie Mellon estimated that the cost to the economy of the time spent reading Internet privacy notices, if they were read, would be $781 billion per year.[14] This is not the way to protect consumer privacy.

To remedy this problem, the FTC proposes that industry provide clear, concise, easy to read, standardized notices. As noted above, SIIA believes that this requirement of universal standardized notice for all information collection other than commonly accepted business practices is the wrong approach. It is also premature. There is an experiment underway with short privacy notices in the financial services industry. The new interagency model privacy notices for the financial services industry became available for use this year. Major financial institutions have already started to use these notices. This test will reveal whether consumers are more likely to read simplified notices and find them useful. FTC should wait to examine the effectiveness of this approach before recommending it more broadly.

SIIA urges the FTC to adopt the principle that the form and content of a privacy notice should be adequate for its intended audience. As the FTC report notes, if the intended audience is teens, the language has to be clear enough for a teenager. If the intended audience is corporate lawyers assessing the privacy practices of a business partner, however, the disclosure can be more complicated. The requirements of clarity in a business context often require the provision of complex detail. In a business to customer transaction notices might need to be simple and concise, but those features might prevent the achievement of the precision that is needed in a business context. There is no need to mandate a standard level of conciseness and simplicity.

Just-in-time notices at the point where consumer is making a decision might be valuable and appropriate in some contexts, but not in others. They might not be technically or administratively feasible in some online and offline contexts. The example in the FTC report of notice at the time of check seems on its face to present insuperable practical difficulties. The durability requirement, in particular, poses significant challenges. To make sure that customers are not presented an indefinite number of times with a choice

[14] Aleecia McDonald and Laurie Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review issue. http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

they have already declined, businesses will need to have some way to re-identify the same customer, which might require the collection and retention of substantial personally identifying information. The FTC appears to acknowledge that the presentation of choice at the appropriate time might depend on the business model. SIIA urges the FTC to build on this insight and recommend a notice regime with substantial flexibility provided to marketplace actors to devise the appropriate form and method for providing notice.

Access

The FTC recommends that customers be given appropriate access to information that companies maintain about them, and singles out especially in this context companies that do not have direct contact with consumers (p. vii). In many cases, such access will be easy and appropriate and will provide benefits both to the data subject and the business. But in other cases, the data will not be kept in a form which is not easily retrievable and the expense of providing the information will not be justified in light of the benefits of access. The FTC recognizes this dependence of an access requirement on the specifics of the context and recommends that the extent of access should be proportional to both the sensitivity of the data and its intended use. SIIA suggests that the FTC build on this notion and make the extent of access subject to a cost-benefit test instead of an absolute requirement.

Section 5 Authority

In several places, the FTC report makes reference to the continued use of its Section 5 authority to prevent deceptive and unfair acts and practices in the area of privacy. This raises the question of whether the framework set out in the report will be used as a standard of unfairness or deception under Section 5. SIIA recommends that the FTC not treat the framework in this fashion

SIIA views the framework that has been developed in the staff report as clear enough as a general guide to information management for business and other collectors and users of information. However, as noted throughout this comment, it lacks precision and clarity at key points. It does not always describe precisely what is required of which businesses in which contexts. This lack of precision at key points makes it unsuitable as a standard to define deception or unfairness in the privacy area.

The FTC's unfairness authority involves the use of a three part test: (1) does the act or practice cause substantial injury to consumers? (2) Can this injury be reasonably avoidable

by consumers? (3) Are there countervailing benefits to consumers or to competition? In effect, this three part test imposes a kind of cost-benefit test on the application of unfairness authority. However, the FTC has not provided any assessment of the costs and benefits of the various practices that it describes in the report. If the FTC intends to use this framework as a standard for Section 5 unfairness cases, it should undertake some economic impact analyses to ascertain whether an information practice is reasonable in light of the benefits it brings to consumers ,to competition and to our domestic and global economies.

Conclusion

Again, thank you for your work on this thorough, thoughtful and timely report. SIIA appreciates the opportunity to comment, and we look forward to working with you on this very important issue. For further information or to discuss these comments, please contact Mark MacCarthy, VP, Public Policy at (202) 789-4471 or mmaccarthy@siia.net, or David LeDuc, Senior Director, Public Policy at (202) 789-4443 or dleduc@siia.net.