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

April 10, 2008

Comments of the

Software & Information Industry Association (SIIA)

To the Federal Trade Commission (FTC)

In response to the FTC's Proposed

"Behavioral Advertising Privacy Principles"

On behalf of the members of the Software & Information Industry Association ("SIIA"), we submit our comments in response to the proposed "Behavioral Advertising Privacy Principles", released on December 20, 2007, by the staff of the Federal Trade Commission (FTC). SIIA appreciates the opportunity to submit our views on the preliminary concepts identified in the staff paper.

As the principal trade association of the software and information content industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

As the FTC is aware, SIIA has been closely monitoring and working with the Commission in the implementation of a number of its policy and enforcement initiatives that touch on this subject area. These areas include, for example, implementation of Section 5 deceptive and unfair trade practices, and the specific initiatives to combat pernicious spyware, promote data security, enforce Gramm-Leach-Bliley, fight identity theft, and implement the Children's Online Privacy Protection Act, CAN-SPAM Act and the Telemarketing Sales Rules (TSR). SIIA was one of the few broad-based industry groups to provide comments prior to the November Town Hall.[1]

[1] Comments of the Software & Information Industry Association (SIIA) on Behavioral Advertising, found at: http://www.ftc.gov/os/comments/behavioraladvertising/071019siia.pdf.

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

SIIA submits these comments from the perspective of many mainstream and well-known brand companies and entities that use and depend on online advertising tools and services to promote and underwrite their own products and services in an increasingly competitive sales environment in which customers are seeking specialized information to inform their purchasing decisions. As such, SIIA members depend on effective and innovative advertising strategies to gain new customers, maintain existing customers and, in many cases, provide a financial basis for new entrants into the market.

Based on our analysis of the document, discussions with FTC staff (which helped to clarify a number of issues and some of the objectives), and experience with the FTC's policy and enforcement effort, SIIA respectfully submits that the proposed principles are a "one-size-fits-all" approach that will not work, as either a basis for further dialogue on self-regulation, or for undertaking enforcement actions. SIIA stands ready to work with the FTC, and with affected stakeholders, to:

- More carefully define the scope of possible activities in this area, including carefully tailoring the terms the FTC is using to reflect its existing policy framework and the reality of the marketplace, and

- Understand and establish the specific harm the FTC seeks to address and tailor any proposed principles to address it.

SIIA and members of our industry commend the FTC for recognizing the key role of self-regulation in this area. Our Association has a consistent record of backing robust self-regulatory approaches, and is committed to do so in the future.

We also note the lack of identification of other steps in the staff proposal that the FTC should consider; in particular, how the FTC can initiate better education of consumers on this issue. Such efforts not only are relevant, but have proven successful in other complex areas, such as spyware and identity theft.

We outline below our view on the limitations and uncertainty of these principles. We look forward to continuing to work with the FTC as it reflects on the comments it receives, particularly regarding the role of advertising and how it is reshaping the fundamental way in which products and services are delivered to customers and creating jobs and new businesses.

While the informal approach taken by the FTC in soliciting comments on the staff document has had the desired effect of stimulating dialogue on this important topic, *SIIA strongly urges that if the FTC intends to establish a basis for engaging self-regulatory efforts or for developing an enforcement framework that it initiate a formal Notice of Proposed Rulemaking procedure to promulgate such principles*.

The Critical Role of Advertising in Today's Economy

Based on our experience in working with the FTC over the last decade on issues affecting Internet commerce, SIIA believes that this area of interest is potentially the most complex that the Commission has faced, and one where precipitous FTC action could be counterproductive.

According to *eMarketer*, a leading industry analysis newsletter, total online advertising spending in the US was estimated to be $21.4 billion in 2007, up from $7.3 billion in 2003. *eMarketer* goes on to report that total online advertising spending in the US will double to $42.0 in 2011.[2] Of this total, search advertising (which includes "contextual text links") was $8.6 billion and expected to reach $16.6 billion in 2001 – about 40% of total online advertising expenditures.[3]

The growing investment in sophisticated advertising is a major contribution to U.S. technology investment and innovation in our industry. A recently released report by SIIA, "Software & Information: Driving the Global Knowledge Economy",[4] documents the critical role that the software and information (S&I) industries, which are increasingly driven by the need to reach customers with new products and services through effective advertising, contribute toward a vibrant and dynamic U.S. economy. For example, the 10.8 percent rate of growth in the S&I industries in recent years significantly outpaces that of the U.S. economy as a whole which climbed by a comparable 3.2 percent GDP. Employees working in the nation's S&I industries are well-compensated, earning among the highest wages in the country. The annual average wage paid in the S&I industries was $75,400 in 2006, 78 percent higher than the average $42,400 for all private-sector workers. Moreover, U.S. firms in our industry are world leaders, selling products and services in markets around the world with strong sales and revenue growth.

In addition to this macroeconomic contribution, Internet advertising has been an essential source of financing for many start-up companies that are working toward longer-term (including subscription-based) revenue models or seeking to get new products and services into the market. Some examples are provided below:

- **Hotchalk.com**. "The HotChalk Learning Environment is community software for teachers, students, and parents. It includes curriculum management, lesson plan development, automated assignment distribution, collection, and grading in a web-based environment. Teachers can find, create and share standards aligned resources and best

[2] Would Microsoft-Yahoo! Mean More Competition?, *eMarketer Newsletter*February 5, 2008, http://www.emarketer.com/Article.aspx?id=1005909&src=article1_newsltr.

[3] Ibid.

[4] Found at: http://www.siia.net/estore/globecon-08.pdf.

practices."[5] The HotChalk Learning Environment is free for all schools everywhere and is based on an advertising-supported business model.[6] HotChalk is working to license and distribute content from larger providers. But without the ability to advertise, HotChalk would not be able to provide its unique services for free to teachers, students and schools.

- **Answers.com.** A "free 'one-stop shop' with instant information on over 4 million topics," Answers.com utilizes an advertising-based revenue model that permits an individual to access reference publications from established publishers to find tailored information.[7] More than a redisseminator, Answers.com provides "original articles researched by Answers.com's in-house editorial team, community-contributed articles from Wikipedia, and user-generated questions & answers from Answers.com's industry-leading WikiAnswers™ (WikiAnswers.com)."

For years, the FTC has recognized the tangible benefits to consumers of accurate, targeted advertising as an effective means to provide choice and competition. The Commission's early reports on the subject[8] laid out many such benefits. Those assessments remain true today, and they have become essential to consumers and businesses:

> "Network advertisers' use of cookies and other technologies to create targeted marketing programs also benefits both consumers and businesses. … targeted advertising allows customers to receive offers and information about goods and services in which they are actually interested. Targeted advertising can also improve a consumer's Web experience simply by ensuring that she is not repeatedly bombarded by the same ads.
>
> "Businesses clearly benefit as well from the ability to target advertising because they avoid wasting advertising dollars marketing themselves to consumers who have no interest in their products. … targeted advertising helps to subsidize free content on the Internet. … advertising revenue helps to subsidize their operations, making it possible to offer free content rather than charging fees for access.
>
> "… profiles can also be used to create new products and services. First, entrepreneurs could use consumer profiles to identify and assess the

[5] "HotChalk Supports Communities of Learners" found at: http://www.hotchalk.com/about.html.

[6] According to HotChalk, with its patent-pending HotChalk Community Standards Engine, each school can control which ads students see, and determine which ads are shown. HotChalk has taken steps to ensure that it never displays advertising during the school day to students. Also children under the age of 13 are never exposed to advertising.

[7] "Answers.com: what we do," found at: http://www.answers.com/main/about_answers.jsp.

[8] See, e.g., "Online Profiling: A Report to Congress", June 2000, found at http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf. (Here in after referred to as "June 2000 Report")

> demand for particular products or services. Second, targeted advertising could help small companies to more effectively break into the market by advertising only to consumers who have an interest in their products or services.
>
> "In sum, targeted advertising can provide numerous benefits to both business and consumers."[9]

The current record confirms that these conclusions by the FTC are true today. In the period of time since the FTC's original report was released, the growth of Internet commerce and the need to reach consumers and end users through the ubiquitous channel of the Internet has magnified these important benefits. Internet advertising is today an inherent element of any company's plan for success.

The personalization of advertising has undergone enormous change in recent years; some even go so far as to suggest a "radical transformation":

> "Gone are the days when marketers randomly placed banner advertisements on related Web sites in the hopes of finding and attracting consumers. With the emergence of today's sophisticated tools and technologies, marketers can now optimally locate consumers at the point of interest in less than a second. As a result, contextual advertising has become an indispensable online marketing tool used to successfully locate and attract consumers on line."[10]

As our industry continues the migration from print-based content to online-delivery of content and related services, companies (and their advertising partners) are increasingly demanding precision in reaching both existing and potential customers. This demand is resulting in new measurements and metrics for determining payments and achieving success in partnering and business relationships.

As a general matter, "Behavioral targeting technologies work by *anonymously* monitoring and tracking the content read and sites visited by a designated unique user or IP as that user surfs the Internet. This is done by serving tracking codes, which are implemented as cookies, on a user's computer as s/he is served ads from various online advertising networks."[11]

---

[9] June 200 Report, pp. 9-10 (footnotes omitted).

[10] Jay Sears, then Vice President of Business Development (now SVP SVP, Strategic Products and Business Development) of ContextWeb, in *Upgrade Magazine* (SIIA), April/May 2005, found at: http://www.contextweb.com/pdf/UpgradeMagazine.pdf.

[11] Loren Baker (Editor of *Search Engine Journal*), "Behavioral Targeting and Contextual Advertising", Sept. 1, 2004, found at: http://www.searchenginejournal.com/behavioral-targeting-and-contextual-advertising/836/. (emphasis added)

However, implementation of this general scheme varies, and new models are appearing regularly. For example, the approach can be applied to "on-site targeting" where the users are segmented based on content views or actions on one site and then are targeted on the site itself. This is distinct from "network targeting" where the users are segmented based on content views or actions on one site and then are targeted where ever they go on sites participating in the behavioral ad network.[12]

As discussed further below (see discussion on the definition of 'advertising'), it is important to recognize that the tools associated with behavioral advertising are also utilized in other contexts, such as news searches (where a reader of one article or series of articles will be able to benefit from additional links to additional articles in the similar subject area) and more generally, in other *non-advertising* content searches.

Preliminary Views on the Proposed Principles

Having reviewed the proposed principles, SIIA continues to urge the FTC, as we did in prior comments before the Town Hall, to consider a careful, tailored approach based on existing policy frameworks, taking into account the rapidly evolving models of Internet advertising and the need to assess the potential benefits relative to the harm.

We note at the outset that the FTC has a strong record and generally well-established approach to enforcing privacy promises,[13] which rely on demarcated understandings and definitions, such as what constitutes personally identifiable information (PII). Reliance on Section 5, of course, is not exclusive; the FTC also has authority based on specific statutory provisions,[14] which all work to provide the FTC with an already existing and workable framework.

With this background, SIIA offers its preliminary views on some of the major issues raised by the proposed principles which point to the need for further work and discussion.

---

[12] "Behavioral Targeting 101," in Web Analysis, Behavioral Targeting and Advertising, Sept. 9, 2006, found at: http://webanalysis.blogspot.com/2006/09/behavioral-targeting-101.html.

[13] "Enforcing Privacy Promises: Enforcing Section 5 of the FTC Act," found at: http://www.ftc.gov/privacy/privacyinitiatives/promises.html. See, especially, *In the Matter of Vision I Properties, LLC, doing business as CartManager International*, FTC Docket No. C-4135 (April 26,2005); and *Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 17, 2004).

[14] See Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

The intended scope of the principles is ambiguous and potentially overbroad. The FTC's focus on "tracking of a consumer's activities online" has generated a great deal of confusion, based on consultation with a wide segment of our industry. The confusion stems from a number of perspectives. For example, is it the intent of the FTC to assume that "tracking" is some combination of collection, maintenance and use of specific information that relates to and is gathered from a particular consumer? This kind of definitional specificity is important since it will be the basis for entities *who will want to responsibly comply with a self-regulatory framework* to adjust their operations and practices accordingly.

In particular, the broad terminology used in the staff paper suggests that the proposed principles are intended to apply to "tracking," *even if it is not collected or obtained directly from the consumer.* This broad scope would then apply to legitimate business practices that are far outside the boundaries of prior FTC actions and policy statements, and which may be developed, maintained or created from a variety of sources, and not directly from the consumer. There is also a practical issue involved: since information that is <u>not</u> collected from the consumer may not be "traceable" in the way that the FTC envisions, implementation of the proposed principles would be impossible to achieve.

SIIA appreciates the discussions with the FTC staff that have helped to clarify some aspects of this issue. We strongly urge the FTC to carefully tailor its focus as it moves forward, including identifying for further discussion and comment the possible set of information that may be collected or "tracked" *directly from the consumer* consistent with the clarifications given by the FTC staff in public forums.

SIIA also strongly urges the FTC to recognize the distinction, referenced previously in our comments, between broad-based Internet behavioral advertising schemes and "on-site" tracking of customer behavior. From the discussions at the Town Hall, and our review of the discussion more broadly, there is no evidence to support the proposition that the kind of concerns expressed by the FTC have been found where "consumer data" is collected and used for advertising within an individual website, or among websites controlled by a single corporate network. In is our strong view, supported by the record, that the FTC enforcement of privacy promises and appropriate security practices provides, in any case, a sound policy framework that is applicable in this regard.

In addition, SIIA strongly urges the FTC not to include "contextual" advertising in the scope of these principles. Where advertising, or information, is provided to a consumer based on the "context" of the content that is displayed on the site, the issues that appear to be of concern to the FTC do not come into play. The risk of confusion for legitimate businesses, however, in this regard is great, since advertising (or other information) is "delivered" and relates to a particular web page being viewed by an individual. However, such context-based advertising does not collect PII or even non-PII. Rather, this model places advertising (or

other information) on the website based on non-individualized elements (usually key words or graphics) displayed on the website.

The "Invisibility Issue". SIIA has carefully listened to the discussions at the Town Hall, examined the proposed principles, and followed the briefings provided by the FTC staff, which has kindly taken the time to engage groups since the staff document was released. To the best of our knowledge, "invisibility" in-and-of-itself is not an actionable item under current FTC law. To restate the law, the FTC Act provides a clear limitation of the Commission's authority: "[t]he Commission shall have no authority under [Section 5] of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[15] The proposed principles appear to be based on general assumptions such as "business and consumer groups alike cherish the values of transparency and consumer autonomy … as critical to development and maintenance of consumer trust in the online marketplace." While hortatory, these type of statements lack a clear basis for understanding the "harm" that is to be addressed.

In terms of specifics, the FTC paper cites "reasonable concerns" about the "possibility" of consumer "data collected for this purpose falling into the wrong hands or being used for unanticipated purposes." We respectfully submit that statements like these need further elaboration from the Commission on what is precisely the injury that the FTC seeks to address, working with industry and other stakeholders, on self-regulatory efforts – particularly when *existing policy frameworks appear capable of addressing and are in fact addressing issues (such as data security practices and enforcement of privacy promises) posited by the FTC.*

The use of the term "consumer data" is novel and lacks specificity. Where use (or misuse) of personally identifiable information poses a direct harm to individuals, the FTC has developed a track record for taking action -- one which SIIA has publicly applauded. Through enforcement actions,[16] as well as consumer education,[17] the FTC has been remarkably consistent in its approach to

---

[15] 15 U.S.C. § 45(n) (2000). *See also International Harvester Co.,* 104 F.T.C. 949, 1061 (1984).

[16] See, e.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.). "ChoicePoint has not implemented reasonable and appropriate measures under the circumstances to maintain and protect the confidentiality and security of ***consumers' personal information***, including a rigorous credentialing process for subscribers to prevent persons without a lawful purpose from obtaining access to consumers' personal information." (para. 31) "ChoicePoint's products and services draw upon billions of records collected and maintained by ChoicePoint that contain the ***personal information of consumers, including names, Social Security numbers, dates of birth, bank and credit card account numbers*** …. (para. 8) (emphasis added in both cases).

[17] **FTC Consumer Alert: Privacy: Tips for Protecting Your Personal Information, found at:** http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.shtm**.** "Each transaction requires you to

focusing on "personal information about yourself." In the process, the FTC has been a leader in shaping a national framework that our industry is relying on and seeking to implement. The proposed principles, however, appear to consciously avoid employing the term "personally identifiable information" and instead use the vague, undefined concept, "consumer data" or "data." We understand from briefings by the FTC staff that this was not intended, but we nonetheless urge the FTC to avoid using this confusing concept.

SIIA is deeply concerned that the FTC staff has indicated in its various briefings that it is prepared to include items that are not *inherently* personally identifiable, such as internet protocol (IP) addresses (among other items). In its discussions, the FTC has asserted developments in the European Union (EU), as well as statements by other federal agencies – such as the Department of Homeland Security (DHS) – to support the argument that IP addresses are to be considered PII. A closer scrutiny of these examples belies the broad assertion that IP addresses are PII.[18]

SIIA emphasizes the need to examine *the specific context in which IP addresses are used*, and avoid categorical conclusions in this regard. Each of the previously mentioned circumstances involves unique statutory and legal obligations, and both deeply involve the question of disclosure of information in the context of *investigations and possible criminal proceedings*, which are not the subject of the FTC inquiry.

In the EU, despite press reports of high profile statements by leading data protection authorities,[19] the actual discussion of the issue revolves around the purpose and manner in which IP addresses may be associated with *other* information that is not collected from the consumer. In the recent high profile case, *Promusicae v. Telefónica,*[20] the European Court of Justice (ECJ) examined the question whether the Internet Service Provider (ISP) Telefónica should be "ordered to disclose the identities and physical addresses of certain persons who it provided with internet access services, *whose IP addresses and data and time of connection were known*"[21] in the context of a civil investigation that included a request for contact information about individuals using the KaZaA file exchange (peer-to-peer) program to exchange pirated sound recordings. Significantly, the

---

share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address and phone numbers."

[18] SIIA notes, as a preliminary matter, that the view of the US government vis-à-vis the European Data Protection law has consistently been that the latter regime is an approach that differs, in many regards, from the approach taken in the United States. As such, reference to developments in the EU, assuming *arguendo* that they are accurate, are not dispositive on the US framework.

[19] *See, e.g.*, "European Regulators Mull Protecting IP Addresses," Information Week, January 23, 2008 06:00 AM, found at: http://www.informationweek.com/internet/showArticle.jhtml?articleID=205916731.

[20] C-275.06, 29 January 2008.

[21] Ibid at para. 30 (emphasis added).

ECJ did not conclude that IP addresses were *inherently* PII as such, because the names and addresses, which did constitute PII, were previously known and linked.

The reference to the view of DHS is also not relevant to the focus of the FTC inquiry on Internet advertising. First and foremost, DHS has not made the categorical determination, at the time of this writing, that IP addresses are inherently to be considered PII, nor that they are PII ***in the context in which the FTC is examining behavioral advertising***. DHS operates under specific statutory authority that authorizes their role in combating terrorism and promoting cybersecurity, as well as other national security and law enforcement responsibilities. Section 208 of the E-Government Act of 2002[22] requires all federal government agencies (including DHS) to conduct Privacy Impact Assessments (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information. In addition, section 222 of the Homeland Security Act[23] requires the Chief Privacy Officer of the Department of Homeland Security to ensure that the technology used by the Department sustains privacy protections. The most recent *Privacy Impact Assessment Guidance2007* includes a definition of PII – *unique to DHS and developed in the context of its government functions and statutory obligations* – as information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, *including any other information which is linked or linkable to that individual*.[24] The "linked or linkable" element relates to the use of information from a variety of sources (including IP addresses and website URL's) by bureaus within DHS that combat cyber attacks and terrorism. For example, the United States Computer Emergency Readiness Team (US-CERT) "builds and enhances our nation's cyber-related situation awareness" by facilitating the identification and coordinated response to cyberthreats and attacks and improvement in network security which *could* utilize IP addresses with other information available to US-CERT to engage in network intrusion detection analysis, and rapid response to denial-of-service attacks.[25]

With this background, SIIA urges the Commission to recognize that in many, if not most, cases the operation of Internet or web-based advertising does not involve the collection, use or maintenance of *personally identifiable information* (as distinct from the function of collecting, using or maintaining PII where it is used, for example, to fulfill a purchasing request). As explained in our pre-Town Hall comments, as a general matter, the Internet advertising tools will utilize randomly

[22] 44 USC 101, et seq (Public Law 107–347).

[23] 6 USC 101, et seq (Public Law 107–296).

[24] *Privacy Impact Assessments Official Guidance*, May, 2007, p. 7 found at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.

[25] Privacy Impact Assessment, *EINSTEIN Program: Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government*, Department of Homeland Security, National Cyber Security Division, US-CERT, September, 2004 p. 1.

generated tracking numbers and segmentation categories that are developed by advertising service providers in conjunction with marketing partners.[26]

SIIA strongly disagrees with the FTC relying on a definition of possible PII that was developed in the context of specific government functions and applicable statutory obligations in the national security and criminal investigation context. The record does not support the FTC assumption that these examples are applicable, or even relevant, to the commercial environment, nor the FTC's conclusion that Internet or web-based advertising tools operate in a manner that raises such a policy question.

The term "advertising" is used generally and lacks specificity. The proposed principles rely on the fundamental premise that behavioral advertising delivers "advertising targeted to the individual consumer's interest." Although the staff proposal includes an allusion to "newspapers and information from around the world," the draft principles lack any discussion of what may or may not constitute "advertising" in this specific context. The establishment of a common definition is more than an academic exercise. It will be a key element to enable entities to know with some predictability what is within the scope of (self-) regulation and how to adjust (as appropriate) business operations and avoiding potential FTC enforcement actions.

We note that these complex issues have been explored in other areas, most notably in the FTC's implementation of the CAN-SPAM Act.[27] Here, the questions are similar: Is the "message" delivered to a consumer in a behavioral context to be considered advertising if it contains only the commercial advertisement or promotion of a product or service? What if the "message" delivered through behavioral display tools includes both commercial content and "transactional or relationship content"? Is the determination of whether the "message" is advertising based on the "reasonable interpretation" of the reader? And, taking into account the FTC's reference to information, if a reader looking at a product online via a website is delivered a review of the product previously published in, for example, *Consumer Reports,* does the delivery of that product review constitute advertising? Is a "message" delivered on behalf of a not-for-profit charity seeking disaster relief contributions to a reader clicking on an article reporting on the effects of a hurricane to be considered "advertising"? These are just a few of the kinds of questions on this point that SIIA looks forward to discussing further with the FTC.

SIIA considers it worth noting that the FTC, in its mandatory rulemaking under the CAN-SPAM Act,[28] appears to have rejected using tests such as whether the

[26] This *behavior* information is distinct from *personally identifiable* information that has been the predicate of FTC enforcement actions to date as part of its "Privacy Agenda."

[27] 15 U.S.C. 7701-7713.

[28] 15 U.S.C. 7702(2)(C).

delivered "message" is supported by other aspects of the advertising regime. Such criteria go to the character of the advertiser – not the particular "message" (which was the focus of the "primary purpose" test under the CAN-SPAM Act). That analysis is relevant here. As reflected in the record during consideration of that Final Rule, use of these kinds of tests may touch on questions of what is permitted speech and first amendment concerns which may go beyond the scope of the FTC's authority to act.[29]

Each of the subjects above is directly relevant to each of the principles outlined. Specific comments on each draft principle follow below.

"**Transparency and Consumer Control."** This draft principle depends heavily on reference to "consumer data", the ambiguous nature of which is discussed above. In the context of generally established understandings of what constitutes PII, it is the view of SIIA that the existing framework of ensuring effective privacy promises is a sound basis for addressing concerns through self-regulation. Through our own educational efforts, SIIA strives to inform members of new developments, and has emphasized that to the degree that PII is being collected in the utilization of behavioral or contextual advertising, this is the kind of disclosure and assurance that privacy policies must provide. Such policies do, of course, indicate if such collection includes an opt-out, and if so, how to exercise it.

SIIA respectfully submits that the FTC has not established on the record that the collection of PII in the delivery of Internet advertising is, in fact, occurring. In the alternative, SIIA respectfully submits that if PII *is being collected*, then the FTC has not established on the record that such collection is in *any* degree different than the collection of PII in other transactions with an individual consumer. SIIA welcomes further discussion to understand how and on what basis the Commission would reach either conclusion. Our industry is well aware of on-going efforts to examine how to improve disclosures, and we welcome that discussion.

SIIA notes the FTC's reference to existing disclosures "as difficult to understand, inaccessible, and overly technical and long." SIIA has followed discussion on this point over the years, and specifically commented to the FTC when the agency undertook its efforts to explore alternative forms of privacy notices.[30] Our

---

[29] This issue was raised in questioning to J. Howard Beales, III, at the time the FTC's Director of the Bureau of Consumer Protection, during the hearing on "Unsolicited Commercial Email" before the Subcommittee on Commerce, Trade and Consumer Protection and the Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce on July 9, 2003. As Director Beales pointed out, the sending of a news alert or article (or we might add, even a full length periodical) – along with advertising that pays for the service – is not meant to be included in the definition of "primary purpose." SIIA believes the same concerns are applicable to the current inquiry. See printed transcript at p. 69. (Transcript available at: http://energycommerce.house.gov/108/action/108-35.pdf.)

[30] See SIIA Letter to FTC on Alternative Forms of Privacy Notices, March 24, 2003, available at: http://www.ftc.gov/os/comments/glbaltprivacynotices/03-31992-0020.pdf.

Association certainly appreciates the desire for "clearer disclosures," and remains committed to working with the FTC and other agencies as efforts are undertaken in this regard. At the same time, consumers should not be confronted with false choices that arise when oversimplification occurs. The record, to date, on simplification has yet to demonstrate that "better" or "clearer" choices are being made by consumers as a result of the interagency initiative.

Consistent with SIIA's previous assessments, we believe the current record indicates that any effort to prescribe the elements, language, format, or mandatory or permissible aspects of a privacy notice has a number of major obstacles to overcome, including the distinct possibility that any such prescription could be a direction that is inconsistent with existing laws at both the state and Federal level. The stark reality is that the FTC does not have exclusive enforcement jurisdiction in this area. Notices provided to consumers, for better or for worse, must address a multitude of issues that could expose an entity to liability.

While it would be convenient to label the challenge as "merely a marketing problem," the practical reality of documenting how personally identifiable information (and even more challenging, how *non*-PII) is collected, maintained and used points to a number of issues that cannot be solved through the micro management of notices. The fact remains that information sharing practices are diverse; and FTC staff has stated in briefings that nothing in this initiative is meant to preclude such practices. Consequently, it is widely recognized by privacy protection authorities and the private sector that "(i)nformation sharing processes can be complex and difficult to describe in simple language."[31]

"Reasonable security, and limited data retention, for consumer data." SIIA recognizes that the FTC has a strong record of enforcement actions and stated policy goals in the area of promoting reasonable security measures. Indeed, the FTC has brought more than a dozen cases[32] alleging that companies misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.[33] In several of the cases, the Commission alleged that the security inadequacies led to breaches that caused

[31] Opening Remarks of FTC Chairman Tim Muris, INTERAGENCY PUBLIC WORKSHOP: GET NOTICED: EFFECTIVE FINANCIAL PRIVACY NOTICES, December 4 2001, Transcript p. 4, available at: http://www.ftc.gov/bcp/workshops/glb/GLBtranscripts.pdf.

[32] *See generally* http://www.ftc.gov/privacy/index.html.

[33] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, Docket No. C-4187 (April 23, 2007); *In the Matter of Nations Title Agency, Inc*., FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.,* FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video,* FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.,* FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.,* FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.,* FTC Docket No. C-4047 (May 8, 2002).

substantial consumer injury and were thus unfair practices under the FTC Act.[34] Some of the cases involved enforcement of the Commission's GLB Act "Safeguards Rule" or the Fair Credit Reporting Act (FCRA).[35] Most recently, the FTC outlined how, even in situations where unauthorized access occurred using sophisticated intrusion strategies and techniques, entities create unnecessary risk to personal information by: storing it on, and transmitting it between and within, its various computer networks in clear text; failing to use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to its networks without authorization; not requiring network administrators and others to use strong passwords or to use different passwords to access different programs, computers, and networks; failing to use readily available security measures, such as firewalls, to limit access among its computers and the Internet; and failing to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as patching or updating anti-virus software.[36]

Similarly, the FTC has undertaken enforcement actions to fight spyware, and initiated at least eight law enforcement actions that successfully challenged the distribution of spyware alleged to cause injury to consumers in the online marketplace[37]

If FTC staff intends this proposed principle to deviate from the existing framework or to add to the obligations of entities, SIIA respectfully requests that the Commission lay out the differences. It is our view that this framework is appropriate and adequate in this regard.

---

[34] E.g., United States v. ChoicePoint, Inc., No. 106-CV-0198 (N.D. Ga.); In the Matter of CardSystems Solutions, Inc., FTC Docket No. C-4168 (Sept. 5, 2006); In the Matter of DSW, Inc., FTC Docket No. C-4157 (March 7, 2006); In the Matter of BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 20, 2005).

[35] *E.g., United States v. ChoicePoint, Inc,*. No. 106-CV-0198 (N.D. Ga.), *supra*, note 14; *In the Matter of Nations Title Agency, Inc*., FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.,* FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services,* FTC Docket No. C-4129 (Jan. 3, 2005).

[36] *In The Matter of The TJX Companies, Inc.*, No. 072-3055 (March 27, 2008, pending final approval by the FTC).

[37] See Federal Trade Commission, Plaintiff, v. ERG Ventures, LLC and d/b/a ERG Ventures, LLC2, Media Motor, Joysticksavers.com, and PrivateinPublic.com, FTC File Nos.: 062-3192 (Oct. 1, 2007); Federal Trade Commission, Plaintiff, v. Digital Enterprises, Inc., d/b/a movieland.com, FTC File No.: 062-3008 (Settlement agreed to, Sept. 11, 2007); *FTC v. Enternet Media, Inc.,* CV05-7777CAS, (C.D. Cal., filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.,* No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com, Inc.,* FTC File No. 042 3196 (filed Sept. 12, 2005), available at http://ftc.gov/os/caselist/0423196/0423196.htm; *FTC v. Trustsoft, Inc.,* Civ. No. H 05 1905 (S.D. Tex May 31, 2005); *FTC v. MaxTheater, Inc.,* File No.: 05-CV-0069 (E.D. Wash. Mar. 8, 2005); *FTC v. Seismic Entertainment, Inc.,* No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

Of course, both the FTC's approach and "data security laws" of states have employed generally consistent definitions of what constitutes PII which if unlawfully accessed or used could led to violations of law and self-help actions. Again, we note the use of the term "consumer data" in this proposed principle is confusing on this issue, and may be inconsistent with the existing legal regimes cited in the FTC staff paper. SIIA, again, urges the FTC to avoid using this novel term.

With regard to data retention, the issue of what is "consumer data" is, again, directly relevant. The FTC's recognition that there may be "good reasons for retaining data" cites only one enforcement area: "criminal activity." As the FTC is aware, its own efforts at enforcement rely entirely on *civil* proceedings – the agency is precluded from bringing criminal charges. This is similar to the options available to the private sector, where data may be retained for a number of legally permissible and entirely appropriate reasons, including bringing civil suit and self-help actions (such as notice and take down measures to combat piracy and counterfeiting, as well as domain name usurpation).

The FTC staff paper also noted other non-enforcement areas, such as "improving customer service." This point cannot be understated. The use of retained data on their customers is critical to their ability to make informed, economic decisions about channel distributions and targeted campaigns, as well as product and service design and implementation. The goal of these strategic initiatives is not simply to permit the retailer to sell more products, but, more importantly, *to engage individual customers in activities about which that customer wants to be engaged* and conversely, not to engage customers in areas where they don't have preferences. Thus, understanding online and offline behavior is critical to effective customer relationship management, and increasingly so in an era of stressed resources.

The FTC paper, however, misses other important functions of retained data. In our industry's experience, appropriate data retention of some variety of elements (including possible PII) may also be essential to combating cyber threats, responding to denial-of-service attacks, fighting web site hijacking, combating phishing emails, and generally promoting network security.

One final point: SIIA urges the FTC to carefully review the draft principles to make sure they work coherently. For example, the security principle applies not only to PII but potentially also to non-PII. In such circumstances, it is the view of SIIA that the first principle (which implies a 'fundamental' level of "choice" be given to a consumer) should not restrict the ability of entities to exercise the proper degree of responsibility, depending on the sensitivity of the information, in carrying out appropriate security practices. In short, security cannot be subject to consumer choice, as the FTC paper has articulated that principle.

"Affirmative express consent for material changes to existing privacy promises." The principle brings into focus two issues: "affirmative express consent" and "material changes." There is a well-developed set of law addressing

consumer consent,[38] which the FTC has over the years acknowledged. Thus, the issue is not addressed directly in the FTC's policy statements, such as "Dot Com Disclosures."[39] If the FTC's use of the language of "affirmative express consent" is in fact another means of raising the question of what is 'clear and conspicuous' (as outlined in section 3 of the "Dot Com Disclosures" statement), SIIA strongly urges r the FTC to explain through a formal Notice and Rulemaking process what this principle entails and how it differentiates from the first principle and well-developed consumer contract law.

The second issue is "material change." The FTC staff paper cites *Gateway Learning Corp*[40] to support this point. The staff paper makes the proposition that a company must keep any promises that it makes with respect to how it will handle or protect consumer data, "*even if it decides to changes its policies at a later date.*" SIIA welcomes further discussion on this point. Our reading of the case is that the *material change* that was at the heart of the alleged deceptive practice was a promise by Gateway that "If at some future time there is a material change to our information usage practices that affect your personally identifiable information, *we will notify you of the relevant changes* on this Site or by email. You will then be able to opt-out of this information usage by sending an e-mail to: webmaster@hop.com."[41] As the FTC complaint the cited case clearly stated, "Respondent [Gateway Learning] … represented, expressly or by implication, that Respondent would notify consumers of material changes to its information practices."[42]

Thus, the FTC alleged that "In truth and in fact, Respondent did not notify consumers of material changes to its information practices. Instead, Respondent posted a revised privacy policy on its Web site without any indication that the policy had materially changed or what aspects of the policy had changed. Therefore, the representation set forth [by Respondent] was, and is, false or misleading."[43]

The "material change" cited by the FTC was, in fact, a deceptive practice, since Gateway Learning did not do what it promised to do. Nothing in the record on Internet advertising supports an FTC interpretation that goes beyond this understanding of what constitutes a "material change." If the FTC intends otherwise, and to include *per se* actions by an entity, SIIA strongly urges that a

---

[38] See, e.g., *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y.2001), *aff'd* 306 F.3d 17 (2nd Cir.2002).

[39] "Dot Com Disclosures," May 2000*, found at:* http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.shtml.

[40] Docket No. C-4120 (Sept. 10, 2004)

[41] Ibid at para. 5 (emphasis added).

[42] Ibid at para. 14.

[43] Ibid at para. 15.

formal Notice and Rulemaking procedure be undertaken to clearly understand the dimensions of this principle and comment effectively.

"Affirmative express consent (or prohibition against) using sensitive data for behavioral advertising." SIIA appreciates the focus of the FTC on this subject, and notes the similar concerns expressed by FTC Commission Jon Leibowitz at the Town Hall as well.[44] Indeed, the examples cited in the FTC staff paper are ones SIIA would recommend for focused further work and discussion. As the discussion is pursued, SIIA notes the use of terms – like "consumer data" – that should be clarified, consistent with the points made earlier in these comments. In each of the examples cited – particularly health conditions and children's activities – SIIA notes that existing legal regimes are relevant (HIPAA and COPPA), as well as existing self-regulatory efforts whose work is recognized by the FTC (CARU).

The FTC Appropriately Recognizes the Role of Self-Regulation

SIIA appreciates the FTC's recognition of the role of self-regulation as a means of promoting confidence in doing business online. In fact, self-regulation has proven to be effective generally in the area of privacy protection, and nothing in the record to date suggests that self-regulation cannot work to address specific concerns that may be identified with regard to implementation of behavioral advertising.

Our Comments submitted today urge continued work in this area, and seek greater clarification on the specific issues that would be necessary to address, if *any* self-regulatory regime is to be created, updated or improved. Without the steps suggested in our comments, the roadblocks to effectuating practical approaches in the area of Internet Advertising will be many.

SIIA does not believe that legislation in this specific subject area is necessary, and we strongly urge the FTC not to advocate such a step.

Conclusion

SIIA looks forward to working with the FTC as these issues are explored further based on the comments received. Please do not hesitate to contact us if we can provide additional information or answer any questions.

---

[44] "So Private, So Public: Individuals, The Internet & The Paradox Of Behavioral Marketing," Remarks of Commissioner Jon Leibowitz at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting & Technology," November 1, 2007, available at: http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf.