



# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

April 11, 2008

**Sent via email: BehavioralMarketingPrinciples@ftc.gov**

Office of the Secretary  
Federal Trade Commission  
Room H-135 (Annex N)  
600 Pennsylvania Avenue  
Washington, DC 20580

Re: Comments on FTC Online Behavioral Advertising Principles

Dear Sirs and Madams:

The Financial Services Roundtable, including BITS, (“Roundtable”) appreciates the opportunity to comment to the Federal Trade Commission (“FTC”) on the proposals set forth in “Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles”.<sup>1</sup>

## **General Comments**

In general, the Roundtable appreciates the FTC’s efforts to raise awareness about issues related to behavioral marketing and to protect the interests of consumers. We recognize that these are not regulatory requirements and the FTC offers these as recommendations for private sector adoption in order to respond to perceived (but not documented) consumer concerns or harm with online behavior advertising. While the title indicates a focus on online behavioral advertising, the draft principles appear to go much further in focusing on fundamental issues of privacy protection and controls, data security practices, and fraud risk management practices.

Additionally, we are concerned that the proposal may take into account all types of information, both personally identifiable information and non-personally identifiable information. Compliance with differing international regulatory requirements is a significant challenge for financial institutions and their customers. Any development of self regulatory principles should be mindful of these differing international requirements. Beyond financial services, efforts are underway to develop cross border

---

<sup>1</sup> The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, investment products and services to the American consumer. Roundtable member companies provide fuel for America’s economic engine accounting directly for \$18.3 trillion in managed assets, \$678 billion in revenue and 2.1 million jobs. BITS is a division of the Roundtable, leveraging intellectual capital to address issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as fraud prevention, critical infrastructure protection, and the safety of financial services.

principles such as those developed by the Asia-Pacific Economic Cooperation (APEC). The FTC should examine these cross border principles when examining this issue.

In light of these concerns, we believe the proposal will evoke a great deal of comment on these other broader issues and not effectively target the specific issue of online behavioral advertising. We are concerned with the broad application of these proposals and the unintended consequences such application may have on the financial services industry, given that financial privacy laws and regulations and best practices among financial institutions already exist in this environment. We believe the FTC should outline the specific harm that these principles would address and then focus on areas where such harm exists.

Financial institutions generally are not directly regulated by the FTC; however, the third party service providers that financial institutions rely on are regulated by the FTC. Thus, we believe these principles could indirectly affect financial institutions. Additionally, we believe that many of the issues raised by these principles are better resolved in other contexts and by other agencies such as financial regulators that have direct authority over the practices of financial institutions. Federal financial regulators have aggressively addressed on-line security and privacy issues through regulations and supervisory guidance over many years. Furthermore, there are a number of initiatives underway to define the appropriate context for using sensitive data.<sup>2</sup> We believe the FTC should defer to the extensive body of existing privacy and security principles – many of which are regulatory or supervisory requirements for financial institutions, as well as voluntary best practices followed by many in the private sector.

Given the complex technologies, market dynamics and policy questions that underlie these principles, this proposal may not achieve workable and effective solutions. We are concerned that they will stifle the online marketplace or needlessly increase regulatory requirements by discouraging relevant and timely advertising messages to a consumer. These are complex issues that require detailed analysis. As such, we recommend that the FTC conduct an in-depth inquiry when examining this issue and work with financial regulators so that any requirements that are adopted are made consistent with financial regulations and supervisory oversight.

### **Clarification on Statutory Authority**

The Roundtable seeks clarification of the authority upon which the FTC relies to promulgate these principles. In the past, the FTC has taken action against egregious cases of on-line behavioral advertising based on its authority under the *Unfair and Deceptive Acts and Practices Act* (“UDAP”). However, UDAP authority would not be sufficient to sustain these guidelines if they were to be made mandatory (e.g., opt-in requirement would be a dramatic change from existing practice and analogous legal rules). We believe that some of the proposals (e.g., opt-in) could do damage by substantially impairing the consumer experience and the ease of use that consumers expect from the Internet.

---

<sup>2</sup> The Roundtable has previously submitted comments in response to other requests for information such as the FTC’s request for input on the use of Social Security Numbers by the private sector, recommendations on the Administration’s Identity Theft Task Force Report, and proposed identity theft “red flags” rule. These letters further demonstrate the extent to which financial institutions have been engaged in protecting consumers through privacy and security practices. See [http://www.fsround.org/policy/regulatory/pdfs/FSRoundtablecomments\\_SSNs\\_090507.pdf](http://www.fsround.org/policy/regulatory/pdfs/FSRoundtablecomments_SSNs_090507.pdf) for a copy of the comment letter on private sector use of Social Security Numbers. See <http://www.bitsinfo.org/downloads/Comment%20letters/BITSRoundtableIDTaskForceLetterFINAL.pdf> for a copy of the comment letter on the Identity Theft Task Force Report recommendations. See <http://www.bitsinfo.org/downloads/Comment%20letters/BITS&RoundtableRedFlagsCommentLetterFINAL.pdf> for a copy of the comment letter on the identity theft “red flags” proposed rule.

Rather, the FTC should base its approach on the *Gramm-Leach-Bliley Act* (“GLBA”), which is the best indication of Congress’ intent to protect financial privacy, and which could be extended to non-financial institutions, at least on a voluntary basis that does not implicate considerations of legal authority. As you know, financial institutions are governed by the GLBA’s Section V provisions on privacy and security. Financial regulators have issued rules and extensive supervisory guidance on many aspects of privacy and security over the past eight years. We strongly believe the balanced, risk-based approach that federal financial regulators have adopted strikes the right balance.

FTC’s current guidance on these principles does not coincide with what now exists in the financial services industry. As such, this guidance would create a number of unintended consequences in the financial services industry, such as increased compliance cost to both businesses and consumers, decreased knowledge about one’s customer, and burdensome account access, creating a negative consumer experience on the Internet. When financial institutions receive complaints from customers concerning their online experience, they adjust their processes accordingly. Additionally, as we discuss below, the current draft guidance may create additional security issues since financial institutions will no longer be able to verify that the customer is exactly who he/she portrays themselves to be.

### **Overly Broad Definition of “Online Behavioral Marketing”**

In responding to the FTC’s request for comments, we are focusing on the activity of behavioral marketing as defined in the Commission’s document. In the industry, online “behavioral advertising” means the tracking of a consumer’s activities online, including the searches the consumer has conducted, the web pages visited, and the content viewed -- in order to deliver advertising targeted to the individual consumer’s interests. However, it appears that the FTC’s proposal includes a broader definition of “behavioral marketing” and essentially defines the term in relation to the use of the information acquired during tracking.

We *recommend* that the FTC limit its scope to tracking and use for marketing purposes, to focus attention to the specific question and avoid peripheral complications. Furthermore, we urge a distinction between cases in which one entity is collecting and using the behavioral information and cases where the collector is different from the advertiser.

### **Specific Comments on Proposed Principles**

#### ***Proposed Principle 1 - Transparency and consumer control***

*Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers’ activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers’ interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.*

We agree that transparency and notice about data collection is fundamental to protecting the privacy of individuals. Notice provides the consumer with information about an organization’s data practices. Notice also requires that firms undertake the internal assessment necessary to write a notice that accurately and comprehensively reflects the company’s practices and makes firms accountable for meeting the standards they set for their own internal practices. Resolving the question about how best to inform the consumer so that he/she may be aware of risks and take actions that are most appropriate to him/her has been a notoriously difficult endeavor. Just last year, federal financial regulators issued for

comment proposed changes to the GLBA privacy notices that financial institutions must provide to customers.<sup>3</sup> Given the difficulty and time it has taken the federal financial regulators to propose changes to a GLBA notice, if the FTC were to create a new notice for consumers, it must gain a better understanding from the industry and the consumers, and it must alert consumers to these new notices.

The Roundtable seeks clarification from the FTC on the harm that the FTC is trying to address with this principle or how technology would work to comply with it. For example, would an organization need to track someone who opted out? If so, would an organization need to track the Internet Protocol (IP) address? Further, it appears that this proposal would mandate an opt-out from targeted advertising delivered and thus an organization would have to be doing some level of tracking to know that an IP address is an opt-out one. Many organizations adhere to Platform for Privacy Preferences Project (P3P) notices – notices which guarantee a certain level of online privacy protection, according to protocol for privacy protection on the Web of the W3C. It is unclear whether adherence to P3P strategies would satisfy this principle.

With both the GLBA privacy notices and the P3P notices, customers are made aware of the collection and use of their information. In today's environment, customers rely on technology to turn off web-tracking devices. This would eliminate the problem posed by this FTC principle of complying with the customers' wishes for the collection and use of their information, while maintaining the type of information that is necessary to process requests and maintain the customers' accounts.

Additionally, the FTC principle appears to require the web sponsor to have the responsibility of disclosure. Placing this responsibility on the web sponsor *vs.* the web tracker or *vice versa* may not accomplish the overarching goal of making customers aware of what information is being collected. For example, a web sponsor should not have the responsibility to disclose or to track opt-outs or opt-ins since the sponsor may not know who is tracking activity on its site, what activity is being tracked, and for what purposes that information will be used. This responsibility may be better suited to the web tracker, which is aware of the information collected and the uses of this information. However, to provide this responsibility to a web tracker may also have some drawbacks due to ever-changing technology. Therefore, the Roundtable *recommends* that this issue be examined further before applying a universal approach.

As we discuss in further detail below, the behavior patterns of an individual are not only important for advertising purposes, but also for fraud and security monitoring. As such, in the financial services industry, the principles may interfere with the legitimate monitoring of an individual's account.

We are concerned that this principle could be interpreted as limiting the collection of any information or could provide an "opt-in" requirement for the secondary use of information. The current approach in the financial services industry is for customers to opt-out. An opt-in approach would be a significant and costly departure from this established approach. Another unintended consequence is that because this proposal does not distinguish among an organization, its affiliates and third parties, these principles could go much further than the GLBA and congressional intent.

---

<sup>3</sup> The Roundtable submitted a comment letter on the proposed changes to the privacy notices in May 2007. See: <http://www.bitsinfo.org/downloads/Comment%20letters/FSRBITSPrivacyShortFormcommentletter.pdf>.

***Proposed Principle 2 - Reasonable security, and limited data retention, for consumer data***

*Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.*

*Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. FTC staff commends recent efforts by some industry members to reduce the time period for which they are retaining data. However, FTC staff seeks comment on whether companies can and should reduce their retention periods further.*

Principle 2 raises two longstanding principles of fair information practices: reasonable security and data retention limitation. While these two principles are important to issues of privacy and behavioral marketing, it is important to recognize that they are not necessarily linked. While it is often argued that limiting the amount of time that data is retained by a company contributes to the overall security of the data, data retention limitation arguably is only one way to enhance security, and in some cases may not promote security at all. To arrive at the best result, the principles of data retention limitation and reasonable security should be uncoupled and each examined separately.

With respect to security, we believe that companies involved in behavioral advertising should be required to provide reasonable security for the data they collect and maintain. We believe the GLBA requirements provide that level of security requirements for financial institutions. Financial institutions have long been required to employ dynamic data protection safeguards to protect sensitive data. The functional financial regulators regularly examine institutions for their compliance with information security and privacy protection safeguards that were included in the GLBA. The FTC and federal financial regulators have already done excellent work in this area in developing the Safeguards Rule pursuant to the GLBA. Recently, the Securities and Exchange Commission issued for public comment amendments to Regulation S-P, which implements certain provisions of GLBA and Fair Credit Reporting Act ("FCRA"). The proposed amendments would set forth more specific requirements for safeguarding information and responding to information security breaches, and broaden the scope of the information covered by Regulation S-P's safeguarding and disposal provisions.<sup>4</sup> Financial institutions have a strong track record in protecting customer information and in deploying robust, risk-based, and dynamic information security programs that include authentication and encryption technologies. Financial institutions continue to develop robust, risk-based and dynamic information security programs including:

- Developing enterprise-wide solutions that take into account the holistic picture and not just specific aspects of identity management and related issues.
- Making authentication easier and more acceptable to users and consumers.
- Applying encryption technology to protect sensitive information.
- Making data more difficult to use even if it is disclosed.
- Educating consumers to use safe on-line computing practices.

---

<sup>4</sup> See <http://www.sec.gov/rules/proposed/2008/34-57427.pdf>.

- Supporting research into customer preferences for authentication (including multi-factor).
- Engaging in discussions among financial institutions and leading software and hardware providers, Internet service providers, law enforcement agencies, and regulatory agencies on how to address cyber security challenges.
- Supporting risk-based approaches for evaluating the risks, deploying controls and offering convenient solutions to consumers.
- Supporting and using the BITS Fraud Program and the Identity Theft Assistance Center (“ITAC”).<sup>5</sup>

Given that many organizations (not just financial institutions) store, transmit or process sensitive information today, all of these organizations should be required to guard this information as stringently as entities compelled by GLBA.

The Roundtable continues to urge legislators and regulators to adopt uniform national standards for both information safeguards and notice on all entities that maintain sensitive consumer information. It is crucial that such standards not be limited to commercial entities, but also apply to other organizations (*e.g.*, universities) that maintain significant amounts of sensitive personal information.

It is important to recognize, however, that questions related to appropriate security have persisted for some time, and businesses’ attempts to grapple with what constitutes “reasonable security” have been ongoing. Decisions about data security are appropriately made based on the nature of the data, the way in which it is intended to be used, and the potential threats to the data. In an environment where business models are dynamic and subject to change, all of these can change, necessitating changes in security.

Technologies available to secure data and systems continue to evolve, as security experts better understand security risks, and act to keep pace with threats. In doing so, data security companies can provide products whose enhanced design reflects changes in the environment. Information-rich businesses must be able to adjust their metrics for security based on these changes and avail themselves of newly developed products that can meet their changing security needs.

With respect to data retention, we believe it is necessary to examine the wide range of considerations companies must undertake to determine the length of time for which data should be retained. Increasingly, organizations recognize that information should only be kept for as long as it has value and can be protected. While this principle urges companies to make these determinations in such a way as to make optimal use of the data but also to minimize the risk to the data, it does not take into account the requirements of business dynamics and a changing market in which appropriate uses for information to meet consumer demand are not immediately apparent.

Further, it will be difficult to resolve this issue without taking into account the ongoing and growing demand of law enforcement for information collected by the private sector. Increasingly, law enforcement requirements play a critical role in determining for how long organizations retain the data they collect. Law enforcement requirements complicate that determination and often place huge burdens

---

<sup>5</sup> See <http://www.bitsinfo.org/downloads/Comment%20letters/BITSRoundtableIDTaskForceLetterFINAL.pdf>. ITAC is an affiliate of the Roundtable dedicated to fighting identity theft through victim assistance, research and law enforcement partnerships. ITAC has helped more than 20,000 consumers restore their financial identities and is the leading source of verified data on identity theft crime.

on companies to keep and relinquish data they would have otherwise disposed. While the broader issue of data retention and law enforcement demands for data are beyond the scope of this FTC inquiry, the FTC must recognize that guidance about data retention policies in the context of behavioral marketing cannot be determined without a thorough vetting of the law enforcement access question.

***Principle 3 - Affirmative express consent for material changes to existing privacy policies***

*As the FTC has made clear in its enforcement and outreach efforts, 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 change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.*

While this principle is, on its face, relatively narrow, we believe it opens a much broader discussion of fundamental privacy expectations. We believe this principle begs the question of what harm the FTC is attempting to address and that any potential harm should drive the definition of “materially different.” We also note that behavior patterns are important not just for advertising but other dynamic, operational priorities such as fraud monitoring, security monitoring, compliance with regulatory or legal requirements and website analytics, where changes are common and often unavoidable. In order for this principle to be operationally effective, the FTC, therefore, would need to articulate a clear, high standard of materiality. Absent this, we believe that the affirmative express consent principle would raise significant issues with respect to potential consumer inconvenience and disruptions of the service models that organizations have developed over many years.

***Principle 4 - Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.***

*Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.*

Principle 4 raises the difficult and persistent question: what constitutes sensitive information? While Congress has acted in certain circumstances to respond to concerns about specific kinds of data -- financial information, medical information, information collected from children -- policymakers have never reached consensus on what information Americans believe is sensitive. Indeed, privacy experts have long held that what may be considered sensitive by one person may not be thought by another to be sensitive. Furthermore, we are beginning to understand that sensitivity is related to the context in which information is being used and the reasonable expectations of the consumer. Some observers have raised the issue of the websites one visits impacting the consumer’s ability to purchase insurance or other risk related products. The Fair Credit Reporting Act covers such uses of information and only requires the FTC to police such activities with enforcement actions. In a sector where the power of analytic tools continues to increase, what was once traditionally considered non-sensitive may become sensitive, when linked. And whether or not information is considered sensitive is also often dependent upon the context and manner in which it is used.

In general, we believe this principle is too vague and could have far reaching consequences. It appears that this principle would limit the collection of any information, but also provide an opt-in requirement for

the secondary use of information. This goes much further than GLBA, which we believe is the appropriate approach, until additional clarity on the policy objective can be achieved. Making decisions about what constitutes sensitive information requires thorough vetting and public discussion. While the solicitation of public comment is a laudable step, it is not a sufficiently robust process upon which to base FTC guidance.

### **Principle 5. Information on Tracking Data for Purposes Other Than Behavior Advertising**

*FTC staff seeks additional information about the potential uses of tracking data beyond behavioral advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.*

The term “secondary uses” is undefined, but the implication in this inquiry is that the use of data beyond behavioral advertising is necessarily of detrimental consequence to the consumer. We believe this is a false premise. It is important to distinguish between the uses of this data for legitimate, often consumer solicited purposes, and the use of the data to “spam” unsuspecting consumers. This proposed principal is so broadly drafted that its adoption will likely result in unduly restricting or possibly even eliminating the beneficial uses of the data. This would certainly be an unintended consequence of using such a broad-brush approach to address an undocumented perception of consumer concern and harm.

Companies use this data for numerous purposes including fraud detection, deterring security breaches, research and development, and improving website design and content. Use of this data in this fashion is of enormous benefit to the consumer, and restricting or eliminating these uses will adversely impact consumers. However, these benefits go far beyond the laudable purpose of maintaining a secure, constantly improving website.

As one example, this data is used to customize the on-line shopping experience to the consumer by permitting targeted delivery of information that is tailored to their individual preferences. Additional examples are endless, but include use of the data to: determine gaps in a customer’s insurance coverage; inform the consumer about relevant and appropriate retirement plans; provide coupons and discounts resulting in financial savings; and allowing a determination of customer preferences resulting in development of improved products responsive to customer needs. The consumer typically consents to these uses either by affirmatively asking for additional information or by continuing to use the company’s web site.

One need only look at the explosive growth of on-line companies to understand that their appropriate, successful use of the information obtained from on-line consumers is something that consumers desire, appreciate and have come to expect. Consumers always speak with their pocketbook, and they are speaking loud and clear about the benefits they derive from the current state of their on-line experience.

### **Conclusion**

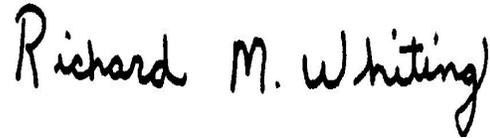
We *urge* the FTC to recognize that the complexity raised by this proposal will require thoughtful, in-depth inquiry and consensus building -- an effort that must extend beyond this request for comments. In the meantime, we believe the requirements laid out in GLBA provide the appropriate security and privacy protection for consumers and should be extended to non-financial institutions. We *encourage* the FTC to be deliberative in its approach, and not rush to solutions that are insufficiently considered and tested.

Thank you for your consideration. If you have any further questions or comments on this matter, please do not hesitate to contact us, John Carlson, or Melissa Netram at (202) 289-4322.

Sincerely,



Leigh Williams  
President  
BITS



Rich Whiting  
Executive Director and General Counsel  
The Financial Services Roundtable