

NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

April 11, 2008

Ms. Jessica Rich
c/o Office of the Secretary
Federal Trade Commission
Room 135-H
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles – Comments.

Dear Ms. Rich:

This comment letter is submitted by the National Business Coalition on E-Commerce and Privacy (“Coalition” or “we”) in response to the Federal Trade Commission (“FTC” or “Commission”)’s Proposed Self-Regulatory Principles (“Principles”) for Online Behavioral Advertising. The FTC has asked commentators to address each proposed Principle and provide additional information regarding the potential uses of tracking data beyond behavioral advertising. This letter sets forth the Coalition’s general comments, followed by its more specific views with respect to each proposed Principle.

I. About the Coalition

Founded in February 2000, the Coalition’s membership includes businesses and associations representing diverse economic sectors, including manufacturing, retail, financial services, and media, and it represents their interests before state, federal, and international policy-makers. The Coalition advocates on behalf of mainstream major American businesses and associations in the areas of electronic commerce and privacy.

The 17 major U.S. corporate and association members of the Coalition are traditional bricks-and-mortar companies now actively using the Internet and new technologies to offer their customers the ability to engage in electronic transactions. Although some of its members are not subject to the Commission’s jurisdiction, the Coalition believes that the FTC’s proposed Principles could well become the basis for an evolving, broader self-regulatory and legislative/regulatory framework affecting all business entities that engage in online advertising, including those not now subject to the FTC’s jurisdiction.

II. General Comments

Behavioral advertising is not a new marketing phenomenon. Prior to the widespread use of the Internet, businesses collected data about consumers in order to more accurately match advertisements, service and product offerings, coupons and promotions to populations with the greatest interest in specific products or services. Now, behavioral advertising provides much of the “information” that is part of the “information economy” and its absence from the marketplace would likely have demonstrable economic consequences. In addition, as discussed in more detail below, the current advertising-related uses of online and offline data are appropriate as is and are already subject to effective and comprehensive federal and self-regulation.

By way of example, the demographic composition of a magazine’s subscriber base or a television show’s viewer base largely determines what advertisements that subscribers and/or viewers ultimately see. This process is designed to provide consumers with products or services more suited to their unique and individualized needs and interests. Likewise, for decades, marketers in the commercial, non-profit and government sectors have used depersonalized demographic information from the U.S. Census to target advertising to consumers via direct mail, television, magazines, billboards, and telemarketing channels. Contrary to the obvious assumption underlying the proposed Principles, to the effect that this invisible collection process is injurious to consumers, we know of no documented or established consumer harm resulting from it. In our view, such harm should be manifest, and an economic impact study performed before any Principles are finalized.

The FTC has indicated that the Principles are based on a “consensus” emanating from the FTC’s November 2007 *Behavioral Advertising: Tracking, Targeting, and Technology* Town Hall meeting (“Town Hall”). We question the presence of such a consensus was present at that Town Hall, and the absence of any kind of summary, formal or otherwise, of what actually took place there, or any kind of objective finding that might reflect the existence of such a consensus, makes any more than an anecdotal reference to a “consensus” impossible. Members of the Coalition who were present at the Town Hall recollect that the only real consensus possibly achieved was an appreciation for the reality that consumers do not generally know nor fully understand how behavioral marketing works. This kind of consensus would perhaps justify a principle that leads industry to engage in more consumer education, rather than a set of principles that pose a potentially dramatic impact on online marketing and do not address offline marketing at all.

At the minimum, any FTC Principles that may result from this initiative should properly balance harm versus benefit. As the Commission itself notes, the benefits of behavioral advertising include “access to newspapers and information from around the world, provided free because it is subsidized by online advertising; tailored ads that facilitate comparison shopping for the specific products that consumers want; and, potentially, a reduction in ads that are irrelevant to consumers’ interest and that may therefore be unwelcome.”¹ Indeed, advertising is what currently makes most Internet content free of cost to the consumer.

¹ See Federal Trade Commission, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (December 20, 2007), <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>, at 2.

Finally, there are other legitimate and legal uses for information related to web user behavior. Applying these Principles could seriously impact the security of users' accounts at financial institutions and put the users at risk of identity theft. For example, a financial institution may use a "flash cookie" or similar digital device placed on an account owner's computer to identify the account owner's particular computer when it is used to return to a website, which, in turn, can allow a financial institution to apply heightened security measures if an attempt is made to access an account from a computer that is not recognized. Some financial institutions may also track web activity in an account to identify unusual account activity for further review (to help determine if the activity is legitimate), secure evidence of unauthorized activity to support investigations by the financial institution and law enforcement, and identify a pattern of behavior for certain types of fraud to determine additional fraud prevention measures that may be appropriate for certain types of financial transactions. In addition, where a financial account has been accessed online in a fraud attempt, a record of web pages accessed in that account would allow the financial institution to determine what information about the account and the account owner has been compromised.

A. The Proposed Principles are Broad in Scope and Not Narrowly Tailored to the Entities or Types of Data Upon Which They Should Focus

As we have noted, the proposed Principles are quite broad in scope. Given the wide-reaching definition of "online behavioral advertising," the Principles would, at a minimum, cover all of the following entities:

- Websites offering the ability for consumers to purchase products and services (first-party advertisers);
- Websites where third-party advertising links are placed;
- Third-party advertiser websites;
- Third-party advertising networks (e.g., members of the Network Advertising Initiative or the Interactive Advertising Bureau);
- Website publishers (e.g., portal websites such as Yahoo!, New York Times);
- Companies that provide website analytics;
- Third-party information publishers; and
- Internet Service Providers (ISPs).

The Coalition wonders whether the FTC actually intends to cover all of these entities, though the ambiguous and inexact nature of the definition necessitates that we assume the broadest possible application.

Further, as discussed in more detail below, the Principles extend well beyond existing laws, regulations and best practices in at least six significant ways:

- Non-PII: Privacy laws, both within the United States and elsewhere, make a clear distinction between personally identifiable information ("PII") and information that is not tied to a particular individual ("non-PII"). The proposed Principles, however, broadly cover the collection and use of all "data"— an undefined term that presumably includes

information that would not qualify under any existing law or regulation as personally identifiable. While protection and safeguarding of all data should be a priority, further restriction of non-PII would mean a significant re-tooling of the systems and technologies used by businesses to manage such data today, at significant potential cost. Thus, the Principles apply to *non-PII*, potentially including log-file data (e.g., IP address, browser type, referring web page) used by the vast majority of commercial websites for both marketing and non-marketing purposes. In practice, most Internet advertising is conducted using non-PII data elements -- e.g., cookies, web beacons, IP addresses -- which are rarely combined with identifying information. No right of privacy attaches to non-PII, and the Principles do not even attempt to articulate why this existing public policy, developed over years of study, as well as Congressional and administrative oversight, should now change.

- **First-Party Marketing (Company-Customer)**: The Principles apply to *first-party marketing relationships* between companies and their customers, not just marketing by third-party advertising service providers. The Principles would therefore far exceed the considered public policy set forth in Title V of the Gramm-Leach-Bliley Act (“GLBA”), as well as self-regulatory regimes adopted by the Direct Marketing Association (“DMA”) and used by most marketers. Under existing law and regulation, companies are free to collect and use information to market to their own customers. In a manner that properly balances consumer protection and business considerations, opt-out choice is required when information is transferred to a third party.
- **Affirmative Consent or “Opt-In”**: The proposed Principle requiring an “opt-in” represents a major change in public policy, and one that equates a change in marketing practices to a material change in a privacy policy. We can find no empirical justification for such a proposal.
- **Affiliate Sharing**: The proposed Principles do not take into consideration that information shared among *affiliated* companies is – and should be – treated differently from information shared with third parties (e.g., as in the GLBA²). Instead, the proposed Principles would regulate all data sharing in the same manner without any substantive justification. The Principles also appear to capture tracking across web pages within a company’s websites, such as a department store’s furniture website and the same company’s shoe website. Companies in different industries – including retail, financial services, travel, and entertainment – often offer different lines of business or brands on separate websites. For example, motion picture distributors’ movie-specific websites also offer descriptions of other movies tailored to movie viewers’ likely interests.
- **Online vs. Offline**: The Principles discriminate against the *online* collection of information, suggesting a stronger regulatory bias against e-commerce, again without any empirical

² Under the GLBA, financial institutions’ privacy policies must provide consumers and customers a way to opt-out of having Non-Public Personal Information (“NPI”) shared with nonaffiliated third parties; no such right exists for disclosure to affiliates except with regards to credit report or application information, per the Fair Credit Reporting Act.

justification for such disparate treatment, and unlike existing and proven U.S. privacy laws (e.g., GLBA and the Fair Credit Reporting Act [“FCRA”]) that apply the same rules equally to both online and offline uses.

- **Collection vs. Use:** The Principles are at odds with existing U.S. privacy laws (e.g., GLBA, FCRA, HIPAA, Do-Not-Call, and CAN-SPAM) that focus on the *uses* of information as the proper area for regulation, as opposed to the *collection* of information. This is a substantial and major change from existing practice and, once again, the Principles are proposed without any justifiable empirical predicate that might explain either the need for a change in public policy or the benefit to the consumer resulting from their eventual adoption. The inevitable result is that the Principles cast a much wider net that captures information flows that pose no demonstrable risk of harm to consumers or anyone else.

The proposal therefore raises the question of whether it is now the FTC’s position that existing privacy laws, regulations, self-regulatory regimes, and best practices are inherently insufficient, absent adoption of these proposals. If existing law and self-regulatory regimes are insufficient, then what do these proposed Principles protect against, and why? Where is the preambular predicate that demands the adoption of such far-reaching solutions?

B. The FTC Should Know What the Likely Economic Impact Will Be

We understand that the FTC’s Bureau of Economics was “involved” in the development of these proposals, but nowhere can we find any analysis of the likely economic consequences of these restrictions, whether self-regulatory or not, on the availability of information in what has developed into an “information economy.” It is disappointing enough that there are no factual or empirical findings to support the promulgation of these Principles, but to move forward with proposals that go well beyond the requirements of existing law and regulation, and to do so without any apparent effort to assess their likely economic effect would be even more troubling. We believe, therefore, that before moving forward in any way with these proposals, the Commission has an obligation to issue a detailed evaluation of what the economic impact would likely be if these Principles were to be universally adopted.

C. Consumer Offerings In Certain Commercial Sectors (e.g., Financial Services) Would Be Adversely Affected

The ability of financial services and other companies to study consumer behavior on websites is critical to their success in serving consumers on the web. These companies use behavior data to improve their online tools and capabilities, to make it ever easier for clients to complete tasks (such as trading, assessing portfolio performance) and to find the information they need (such as CD rates and availability). If financial services companies are prevented from accessing behavioral data, they would have to rely on surveys and in-person interviews/usability tests. These alternatives are less effective, and will likely result in a less desirable and a less productive experience for consumers.

Financial services offerings are complex, and consumers benefit from receiving targeted information and a tailored experience that is relevant to their situation and needs. For example, financial brokerage firms provide their more active traders with specific tools and information that are suitable for a more sophisticated trader, but could be confusing for a more novice investor. Financial services companies use information about tasks that a website visitor has just completed to suggest appropriate next steps. If such companies were not able to provide segmented, targeted experiences, they would need to provide a more generalized experience for all site visitors, which would be significantly less user-friendly and would not adequately meet consumers' specific needs. Many financial services clients also visit and browse a website several times before purchasing a product or service. The use of behavioral data by financial services companies allows the company to better tailor the experience for return shoppers and helps customize and focus their shopping experience.

D. The Principles Discriminate against Online Commerce

In the offline world, businesses sometimes share information about consumer transactions with third parties. This type of sharing is usually regulated either by the GLBA or the DMA self-regulatory standards, both of which require that consumers be provided notice and an opportunity to opt-out. The Commission has not provided any rationale for imposing a different set of principles in the online world. Why should e-commerce practices be treated differently than the offline practices that have existed for years? If consumers are harmed by one, then it follows that they are harmed by both. Accordingly, the Commission should explain its rationale for this discriminatory treatment.

E. Any Online Behavioral Advertising Principles Must Weigh the Consumer Benefits against Consumer Harms

At the Town Hall, FTC officials conceded that it is unclear whether or not behavioral marketing has resulted in any consumer harm or is likely to do so in the future. The FTC expressed its commitment then to study the issue and report back to industry, although, as noted below, it has not yet produced any evidence that consumer harm has resulted from existing practices, nor does it demonstrate why existing laws and regulations are insufficient to address those instances in which data is misused.³ On the flip side, as the FTC Staff Statement on Behavioral Advertising readily acknowledges, behavioral advertising on the Internet provides significant consumer benefits. It is central to the availability of free, quality content on the Internet and to useful

³ Consumer groups (as well as the FTC, in meetings) point to a breach of AOL user search requests, which contained information that could be traced to individuals as an example of potential harm. However, this was, in reality, a data security problem, and AOL notified those individuals about whom personally-identifiable information was exposed, as a best practice and in line with existing state laws and FTC settlements with other companies. We know of no harm that came from this data breach, and certainly the breach alone, absent more, does not justify the far-reaching Principles the FTC has proposed. Perhaps more importantly, the AOL data that was breached was in no way related to "online advertising" information. Search engine keywords were not being used by AOL to display subsequent advertisements to those respondents.

comparative advertising. It also provides Internet users with advertisements in which they are more likely to be interested, and fewer ads that are not of interest.

We respectfully request that the Commission not proceed with these Principles, in the absence of an empirical foundation – including an economic impact assessment to justify the proposals. In the absence of such a record or finding, the Coalition is currently handicapped in its effort to responsibly consider and comment upon the efficacy of the FTC’s proposals, to test the Commission’s presumptions, or to search for real-world examples of harm and, if such real-world harms are discovered, to suggest workable alternative solutions for the FTC’s consideration.

Moreover, Congress has not enacted legislation that would provide the FTC with regulatory authority in the behavioral advertising area, and issuing “self-regulatory” Principles that expand beyond those boundaries is inappropriate. Past FTC “Principles” have been based on the FTC’s authority under Section 5 of the FTC Act or the record upon which it based its enforcement actions. For example, in March 2007, the FTC released the publication *Protecting Personal Information: A Guide for Business*. The publication sets forth specific recommendations such as “Use Social Security numbers only for required and lawful purposes – like reporting employee taxes.” While directed at improving business practices without resorting to regulatory or enforcement measures, these principles fall into the same area – data security protection – in which the FTC has had extensive experience and significant enforcement authority by virtue of its closely related work implementing the GLBA Safeguards Rules and enforcement of Section 5 of the FTC Act. By contrast, Congress has neither introduced nor enacted legislation in the behavioral advertising area, nor does the FTC have the benefit of past enforcement actions to guide its Principles (although the Commission has conducted merger reviews indirectly relating to behavioral advertising).⁴

In our judgment, any proposal of this breadth and impact promoted by an enforcement agency with the well-deserved reputation of the Commission must weigh the consumer harms against the benefits, and must be accompanied at least by an explanation of the established public policy need as well as a justification for why it must be seriously considered. We see no empirical evidence that these Principles are accompanied by either.

III. Specific Proposed Principles

A. 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

⁴ The FTC has also issued “Green Guides” that are intended to describe the application of Section 5 of the FTC Act to environmental advertising claims and practices. The guides were published in response to petitions from companies and trade associations, recommendations from state Attorneys General, public hearings, and public comments. While the Principles were similarly developed from public comments, industry workshops, town hall meetings, and the FTC’s own official statements, we feel that there is much less justification in this case to issue Principles than in the examples cited above. Here, there is no evidence of actual harm, recommendations from state law enforcement bodies, or a clear nexus with existing statutory authority.

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.

The Coalition generally supports this Principle, but it is entirely too broad in scope. Coalition members already provide clear, concise, consumer-friendly and prominent privacy notices that address their online information collection practices and allow consumers to opt-out of having PII shared with unaffiliated third parties for marketing purposes, where required. Unlike the GLBA, a federal statute supported by robust debate and legislative history, this Principle does not appear to take into consideration how information shared among *affiliated* companies should be treated. Rather, it would regulate all data sharing in the same manner, without any distinctions. Importantly, there are currently no laws, self-regulatory regimes or best practices that would require website operators to provide an opt-out for information collected about the consumer.

In addition, the Coalition questions why existing self-regulatory principles, including those developed by the Network Advertising Initiative (“NAI”) and Interactive Advertising Bureau, (“IAB”) are insufficient. As discussed above, the FTC cites no record to support the determination that existing self-regulatory principles do not adequately protect consumers. Further, although concern has been expressed that the NAI Principles have not been enforced, the Coalition questions why the FTC cannot simply exercise its enforcement power to enforce companies’ pledges to abide by such principles. Rather than adopting new Principles, the FTC should use its existing authority under Section 5 of the FTC Act to enforce compliance with existing self-regulatory regimes.

B. 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.

The Coalition has long advocated this Principle - as securing personal data is an existing moral and common law obligation for any entity that has custody of such data - but it should be made consistent with existing law. Coalition members already use data security measures and best practices consistent with GLBA, the GLBA *Safeguards Rule*, the FTC's *Disposal Rule*, the *Interagency Identity Theft Red Flags and Address Discrepancies Joint Final Rules and Guidelines* (implementing FACTA), as well as state data destruction and security laws. This Principle should be re-written in a way that is clearly in line with existing law.

C. 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.

Once again, the Coalition supports this Principle in theory, but limiting the retention of information to a set period of time would be both impractical and unwarranted. Our members

already retain information for only so long as business needs require them to. Business needs are imprecise, however, and a time period that might apply to one business model might well be insufficient to meet the needs of another model. As a general premise, this Principle both makes sense and is already in effect, but as is the case so often with these proposals, it is unclear whether the Commission anticipates a set period of time that a company can hold such data. In addition, legal and regulatory requirements—such as varying state statutes of limitation and regulatory record retention obligations—would need to be taken into consideration.

D. 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.

The Coalition strongly agrees that companies should be precluded from reneging on promises made in their privacy policies in a way that directly impacts consumers who provided personal information based on that representation. Nevertheless, we believe that if this Principle were adopted, businesses will be less inclined to make robust and clear disclosures in their privacy policies for fear that any such “change” might be considered an alteration of existing practices resulting in significant and burdensome operational challenges.

As when data is transferred in the offline world, consumers should be provided with a robust notice and an opportunity to **opt-out**, where required, before personal information pertaining to them is transferred to an unaffiliated third party for marketing purposes. Coalition members, and other reputable companies, already maintain internal opt-out files for consumers who do not want to receive marketing materials. If a company changes its policy from “not marketing” to its customers to one of “marketing to” its customers, these internal opt-out files ensure that no marketing materials are sent to those customers who do not wish to receive them.

On the other hand, applying an opt-in rule to data transfers associated with a corporate merger, bankruptcy or similar legal proceeding, where the company with custody of the data has made no pledge that such data would **never** be transferred, is unworkable in situations where consumers have changed addresses or otherwise cannot be located. Such situations are common, and might result in a significant delay to the transaction or to a bankruptcy proceeding.

Furthermore, this proposed Principle appears to be based on a misinterpretation of the *Gateway Learning* consent decree. The *Gateway Learning* case, Dkt. No. C-4120 (Sept. 10, 2004), did not indicate that material changes to **any** internal data collection practices trigger an opt-in requirement. On the contrary, *Gateway Learning* involved a company’s pledge *never to disclose personally identifiable information*. Subsequently, the company unilaterally changed this policy. *None* of these conditions are mentioned in this proposed Principle. Rather, it appears to assume that entities that have not made these kinds of unilateral promises are collecting non-personally identifiable data, are not disclosing any PII to third parties, and should obtain affirmative consent

before changing their practices. In fact, far from suggesting this sort of rigid rule, *Gateway Learning* suggests a “sliding scale” under which notice, notice and opt-out, and affirmative consent may be required in different circumstances.

In sum, a change in internal business practices should not itself equate to a material change, and this type of policy change may create disincentives for businesses in terms of the disclosures they make in their privacy policies.

E. Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. The FTC 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.

(1) What classes of information should be considered sensitive?

The Coalition agrees there may be certain sensitive data elements that should not be used for behavioral advertising, absent affirmative express consent. For example, there may be certain types of health and financial information that fall into this category. Others might include sexual orientation and information pertaining to sexual content. On the other hand, non-PII has never, under any legal regime, been considered “sensitive.”

Determining which kinds of data are sensitive for purposes of behavioral advertising depends to a great deal on consumer expectations. For example, if a consumer visits a website offering multi-vitamins, he or she will expect (and certainly wouldn’t be surprised) to see an advertisement on the side of the page for iron supplements. The consumer might be surprised, however, to see an advertisement for high-definition television.

(2) Should using sensitive data for behavioral targeting not be permitted, rather than subject to consumer choice?

As stated above, the Coalition believes that using sensitive data for behavioral targeting should be subject to consumer choice. The Commission notes, however, that an opt-in standard may not be appropriate for the **collection** of information that may be considered sensitive, as opposed to the use of such information. In addition, the uses of certain types of sensitive data – such as children’s PII and personal health information – are already regulated under existing law. Thus, the Coalition questions how this Principle would mesh with existing law.

The Commission certainly has reason to engage further with groups that administer self-regulatory regimes to identify specific data elements that should be considered sensitive, and the Coalition would be pleased to participate in this effort.

IV. Call for Additional Information: Using Tracking Data for Purposes Other Than Behavioral 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.

(1) Which secondary uses raise concerns?

Our comments here depend on whether the FTC believes that the use of data for behavioral advertising is itself a secondary use; the Principles do not say. The Coalition's membership believes that once notice is provided to the consumer, and an opportunity to selectively preclude the transfer of PII to third parties is provided by way of an "opt-out," the data collected may be used for a range of secondary purposes, so long as those purposes do not expose the consumer to a greater risk of identity theft and/or financial account fraud. If one of the secondary uses is to deliver custom-tailored information about specific products and services, then the consumer benefits. If another is to more effectively devote research and development resources to products and services more tailored to the consumer's needs, then the consumer again benefits. If another is to segment the marketplace so as to customize corporate advertising, then we believe the consumer once again benefits. Ultimately, what qualifies as a secondary purpose drives the conclusion, and all secondary purposes should not be deemed suspect.

(2) Are companies in fact using data for these secondary purposes?

Companies may use tracking data to perform various tasks related to their websites, such as:

(1) Banner advertising messages – here, entities might collect data indicating which web pages were viewed by particular visitors. The data is collected to affect the likelihood that specific marketing messages are received by consumers who find them useful. For example, if a website visitor has visited a page describing a fixed income offering, then it is more likely that the website visitor will see messages promoting fixed income products and research;

(2) Custom site content (not advertising banners) – again, entities might collect data indicating which web pages were viewed by a certain visitor and the referral "source" web page. This data is collected to provide the website visitor with the most relevant content in certain areas of the site, depending on the expressed intent of the visitor. The practice of customizing site content is designed to help the visitor find the content/information he is looking for more easily; or

(3) Site design and content development – non-PII data, such as the web pages or links where website visitors enter the site, which web pages were viewed, and the places where visitors left the site, might be collected. This data is used to optimize the site's design, make common tasks easier to complete and to clear obstacles from key navigational paths.

(4) Subpoenas/law enforcement requests – law enforcement or government entities sometimes issue subpoenas. However, in order to obtain tracking data, these subpoenas would need to specifically request a consumer’s website behavioral or tracking information. Even if a law enforcement agency were seeking this information, most online services and websites use dynamic tracking mechanisms per website “session,” which cannot be easily tied to a particular individual. In such cases, the subpoena would have to require the online service provider or website operator to produce logs indicating all of the tracking mechanisms (e.g., cookies) used and whether any such mechanisms could have been assigned to a particular individual on a given date/time. Even if all of these conditions were met, a consumer would have been made aware of the possibility that this type of disclosure might be made. Online privacy policies usually state that PII might be shared when required by law or pursuant to valid legal processes.

In addition, entities may use tracking data for legitimate, lawful purposes unrelated to behavioral advertising. Such legitimate “secondary uses” include:

- (1) responding to law enforcement requests (see discussion above);
- (2) fraud detection and prevention;
- (3) identity verification; and
- (4) market research

Thus, companies often use online technology in their fraud detection and prevention programs to track user behavior and apply rules to locate unusual patterns in a user’s behavior that might indicate that fraudulent activity is taking place. Technology that tracks user behavior is therefore a valuable fraud prevention tool because it occurs without alerting fraudsters as to how the system’s logic works, making it more difficult for fraudsters to learn and evolve. These online technologies are capable of intervening when a rule is triggered to require more in-depth authentication from a user. If companies are limited in their ability to track and store information regarding previous online behavior, the core capability of these anti-fraud systems – i.e., to track behavior over time and learn to locate anomalies in that behavior – would be severely restricted.

(4) Do secondary uses, if they occur, merit some form of heightened protection?

The Coalition questions why tracking data should receive a higher level of protection than other types of consumer data. The uses of other types of consumer data – e.g., consumer report information used for determining eligibility for credit, employment or insurance – are already highly regulated under federal law. Likewise, the use of nonpublic financial information is already regulated under federal and state law.

In addition, it does not make sense and is unworkable for restrictions on “secondary uses” to apply to intra-company uses – for example, the sharing of such data amongst affiliates of the same company (see Section II.A above).

V. Conclusion

We very much appreciate the opportunity to comment on the FTC's proposed Principles, and are anxious to work with the Commission as it contemplates its next steps. We hope that our comments have been helpful and we wish to contribute to whatever comes next. If you have any questions or need any additional information, please do not hesitate to contact me at 202.799.4361.

Sincerely,

A handwritten signature in black ink, appearing to read "Tom Boyd". The signature is written in a cursive, slightly slanted style.

Thomas M. Boyd
Counsel