



Wells Fargo & Company
420 Montgomery Street
San Francisco, CA 94104

April 10, 2008

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

Email address: BehavioralMarketingPrinciples@ftc.gov

Submitted via overnight delivery and email

Re: Proposal entitled “Online Behavioral Advertising/Moving the Discussion Forward to Possible Self-Regulatory Principles”

Dear Sirs and Madams:

This letter is submitted on behalf of Wells Fargo & Company and its affiliates (“Wells Fargo”) in response to the Federal Trade Commission’s (“Commission”) proposal entitled “Online Behavioral Advertising/Moving the Discussion Forward to Possible Self-Regulatory Principles” (“Proposed Principles”). Wells Fargo appreciates the opportunity to comment on the Proposed Principles.

I. Summary

Wells Fargo appreciates the Commission’s attention to the important issue of online behavioral advertising (“OBA”). But there were flaws in the process resulting in issuance of the Proposed Principles, which in turn contributed to serious defects in the substance of the document.

With regard to procedure, before any self-regulatory principles are announced — either by a governmental agency or industry itself — existing law and regulation should be examined. In issuing the Proposed Principles, the Commission skipped this important step.

Further, by its nature, self-regulation should be developed by the businesses to which the standards would apply, rather than imposed by the government. To determine whether additional self-regulation is necessary in this area, entities that maintain self-regulatory standards should first evaluate and articulate consumer harm and concerns that self-regulation may need to address further. This step did not occur.

Last with regard to procedure, notably absent is any detailed analysis of how, if at all, the Proposed Principles actually further traditional consumer privacy interests.

With regard to the substance of the Proposed Principles, Wells Fargo respects the Proposed Principles' effort to balance consumers' dual interests in privacy protection and in support for online innovation that benefits consumers. But substantive aspects of the Principles too heavily impair consumer-friendly innovation and a customized, rich online experience for consumers without materially advancing any consumer privacy interests.

To more optimally protect consumers' interests in (1) transparency and clarity of practices; (2) privacy, including security and limited distribution of various kinds of data; and (3) internet usability and innovation, the Commission should reassess the Proposed Principles. Even at this early stage, when the above critical steps in the process have not been undertaken, it is clear that at a minimum, the following substantive modifications would have to be made to any revised principles:

Overarching issue: neither the definition of OBA nor any of the Proposed Principles distinguish between personally identifiable information and non-personally identifiable information. These two types of information deserve distinct treatment since there has been no articulation of how non-personally identifiable information implicates privacy concerns.

The definition of OBA must be substantially revised to include only true "online behavioral advertising" where information is collected across third-party websites to predict consumer characteristics or preferences to deliver advertising online. All of the following should be excluded from the definition of OBA:

- Information collected and used only by one site, or a family of sites operated by affiliates.
- Advertisements delivered based on information affirmatively inputted by a user.
- "Context-based" advertisements delivered uniformly to all users visiting a site or certain content.
- Last, the phrase "the searches the consumer has conducted," which is currently included in the OBA definition, should be eliminated.

Principle 1 (notice of practices and provision of "opt-out"): The portion of Proposed Principle 1 that calls for clear and accurate disclosure of OBA practices should be

retained. However, the second portion of this principle, involving provision of an “opt-out,” should be eliminated unless and until further substantial consideration is given to the numerous ways in which this portion of the first Proposed Principle might detrimentally affect consumers.

Principle 2 (data security and retention): The data security provision should be retained, but the data retention portion of the second principle should be modified to allow for more flexibility for reasonable data retention practices.

Principle 3 (“Affirmative express consent for material changes to existing privacy promises”): Without substantial revision, this Proposed Principle should be abandoned and not issued at all. The current draft must be modified to make clear that the principle applies only to material changes to existing privacy promises *with respect to OBA*, and not to privacy promises regarding other practices, such as use of information for servicing an account or an entity using its own information about a customer to deliver customized content or advertising. Even if so limited, as in other areas, any principle announced with regard to privacy notices should be inapplicable by its own terms when existing law already applies to an entity or practice. The current draft would also be aberrant in calling for an “opt-in” rather than an “opt-out” standard for changes to privacy notices. Last, this principle would also be detrimental to informed consumer choice, as it would provide an incentive to companies to announce to consumers the least protective practices that are allowed by law.

Principle 4 (“opt-in” requirement, or ban on, using “sensitive data” for OBA): The term “sensitive data” is not defined. Without definition, the current principle is simply too vague. Additionally, when and if this term is defined, to the extent that the definition covers information already subject to existing law or self-regulation, that law and/or self-regulation should apply to such information, rather than piling on a potentially confusing additional layer of requirements. As written, the Principle furthers no consumer privacy interests. Indeed, the suggestion of a complete ban on the use of “sensitive” data is extremely hostile to consumers’ ability to access information. Even an “opt-in” regime would be so unwieldy as to threaten many extremely popular internet functionalities, such as basic search engines. Without all of these issues addressed, Principle 4 should simply be subsumed within Principle 1, such that Principle 1 would cover both “sensitive” data and data that is not “sensitive” or that is less “sensitive.”

Section 5 (request for information on “secondary uses” of “tracking data”): There are many “secondary uses” of what the Commission calls “tracking data.” Information gathered is used for many purposes besides delivering targeted advertising, including: authentication and other internet security measures; to allow a website to recognize an IP address, such as to deliver customized home pages on portals, and to retain information on certain sites to deliver customized functionality; to facilitate research to improve navigability and usability of sites; and to determine the popularity of certain sites or site content. For the reasons set forth below, none of these purposes raise any heightened concerns.

II. Background Regarding: Selected Existing Statutes and Regulations; Self-Regulation; Traditional Privacy Values and Principles; and the Commission's Concerns

The various activities that constitute OBA (as defined in the Proposed Principles) are relatively new practices in a relatively new medium. To facilitate development of sound, well-reasoned, and consumer-friendly principles in this arena, the Proposed Principles should be evaluated in light of existing legal requirements, existing self-regulatory regimes, and traditional and core privacy values. In this section, we briefly give a background on existing statutory and regulatory regimes, on existing self-regulatory principles, and on bedrock privacy principles. We also set forth the Commission's concerns with OBA. In the sections that follow, we analyze the degree to which aspects of the Proposed Principles may conflict or overlap with existing statutory and legal frameworks. We also analyze the degree to which the Proposed Principles either do or do not advance core consumer privacy interests and either would or would not truly address the Commission's concerns. We highlight where certain language of the Proposed Principles furthers consumer privacy and other interests and thus should be retained. We also point out where certain aspects of the Proposed Principles may superficially appear to further some consumer interest, but explain that these portions do not advance any real privacy interest but instead impair other consumer interests, such as internet functionality and customization. In such instances, we urge specific modifications to the Proposed Principles.

A. Selected Existing Statutes and Regulation

Before any self-regulation is issued, existing law and regulation should be examined. There are several reasons for such an investigation. First, if law or regulation already governs a practice, then no self-regulation is needed, and indeed, self-regulation may conflict with law. Under this scenario, self-regulation may in fact confuse businesses and consumers alike. Second, to the extent that there are gaps in law and regulation, such as coverage of certain entities (e.g., financial institutions) but not others, learning from existing law and regulation could inform what type of self-regulation for uncovered entities or practices would be most effective. Third, any self-regulation should also make it clear that as to entities that are subject to current laws and regulation in the OBA area, those existing laws and regulations apply as to those entities rather than the self-regulatory principles.

As relevant here, financial institutions are governed by the privacy and security provisions in the Gramm Leach Bliley Act, 15 U.S.C. §§ 6801 *et seq.* ("GLBA"). 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 between benefit and risk to consumers and financial institutions. We detail below certain instances in which the Proposed Principles may be inconsistent with existing law and regulation applicable to financial institutions. We highlight where the Commission should conform any principles to the existing statutory and regulatory

authority. We also urge that, to the extent that any inconsistent principles are adopted, the Commission should make clear that they do not apply to institutions already governed by statutory and regulatory authority.

B. Existing Self-Regulation

Wells Fargo believes that effective self-regulation allows for flexibility and adaptability in responding to changes in markets, business practices, technological advances and, importantly, consumer expectations. Similarly, self-regulation is particularly effective in the internet medium where innovation is exceptionally rapid and consumer response swift, and business continues to demonstrate an ability and willingness to adapt self-regulatory frameworks to issues as they emerge.

Any assessment of the need for additional self-regulation should carefully examine existing frameworks and determine whether they are sufficient and, if not, in what areas additional practices should be adopted. We understand that various groups with existing self-regulatory regimes are engaged in such a process. In considering any revised principles, the Commission should consider the results of such an examination, issuing any principles only to address any documented, substantial concerns with existing self-regulatory and legal regimes.

C. Traditional Privacy Values and Legal Theories

The core privacy interests and principles that underlie law and regulation are based on the traditional four common law privacy torts:

- ***“Public disclosure of private facts”***: This tort operates to restrict disclosure to the public, or to a larger number of persons such that the information can be deemed to be publicly distributed, of certain personally identifiable information. (The GLBA can be viewed to have grown out of the interests protected by this tort, as the GLBA operates to restrict financial institutions’ disclosure of nonpublic personal information.)

- ***“Intrusion upon seclusion”***: A physical or other type of intrusion upon the solitude or seclusion of an individual or his or her private affairs or seclusion. (Telemarketing laws allowing an individual to restrict a company or companies from telephoning the individual are an example of the type of interest protected by this tort.)

- ***Being presented in a “false light” to the public***; e.g., publicizing a newspaper story about individual X in which certain of the statements that are made are true but in which details about the person are also invented that are not true.

- ***Misappropriation of one’s name or likeness***; e.g., an individual’s name is used without permission to falsely imply that the individual has endorsed a product

D. Unfair and Deceptive Acts and Practices Principles

As the Commission has often recognized, and as acknowledged by certain portions of Proposed Principle 1, *unfair and deceptive acts and practices principles* may also arise with regard to privacy practices. Business practices affecting privacy interests should be clearly and accurately conveyed to consumers.

E. The Commission's Concerns with OBA

The Commission points to three specific concerns with OBA:

- the practice itself is largely invisible and unknown to consumers
- consumers do not understand the role that data collection plays in OBA
- a potential that consumer data collected for OBA will fall into the “wrong hands” or be used for “unanticipated purposes”

III. The Proposed Principles Underestimate the Savvy of Many Internet Users

Contrary to the Proposed Principles' implication, it strains credulity to believe that many users are unaware of practices that fall within the Proposed Principles' definition of OBA. Many users understand, for example, that: Google AdWords are the result of the search the user input; advertisements that many of the various commercial websites deliver are based on the search that the user input (e.g., search on target.com for socks delivers product content based on that term) or other content viewed (e.g., amazon.com suggests additional products based on products viewed); and advertisements that a site delivers are sometimes based on the content showing on the screen (an ad for a particular pet food shown on a screen with content about proper care for a pet).

IV. The Definition of “Online Behavioral Advertising” Is Overly Blunt and Broad

The Proposed Principles broadly define OBA “to encompass the various tracking activities engaged in by diverse companies across the Web.” Specifically, OBA is “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.” As currently drafted, the Proposed Principles are too blunt of an instrument to deal with OBA, as so broadly defined.

- *The OBA definition should not apply to information practices within a site or family of sites under common ownership or control.* The OBA definition should apply only to information collected over time and across third-party sites, and not to information collected at an individual site or within a family of sites owned by the same corporate entity. We believe that consumers are aware of and significantly benefit from use of information from first-party websites. Such information is not the type of so-called “invisible tracking” where consumers are unaware of the entity that is collecting

the information. Consumers are unlikely to be confused — indeed, they are likely to understand and appreciate — that a single site will use information gathered solely at that site to help deliver relevant content on that site. For example, a consumer would be unlikely to be surprised or confused by an online bookseller delivering content about new releases in mysteries, when prior content viewed on that site showed an interest in that genre. This is a well-known practice that consumers have broadly adopted and from which they have benefited. Similarly, as described below, website privacy policies have proven to be a very effective means for consumers to understand their interactions with a website.

- ***Personally identifiable information (PII) as compared with non-personally identifiable information (non-PII).*** The definition does not distinguish between OBA that is based, in whole or in part, on personally identifiable information (“PII”) as compared with OBA that is based solely on non-personally identifiable information (“non-PII”).

- ***Elimination of “including.”*** The word “including” in the current definition is unbounded and, as a result, could include any type of information collected online and used to deliver advertising. Such a sweeping approach is inappropriate and could unnecessarily interfere with critical business practices.

- ***Transaction or other information affirmatively inputted by a consumer should be outside the scope of OBA.*** Any information that is directly provided by the consumer and not passively collected should fall outside the scope of the definition of OBA. Transactional and other similarly collected information entered by the consumer already is effectively governed by the privacy notices of companies, including online privacy notices, where consumers are told how the information will be used and provided choices for such use. Such notices have been widely adopted. For example, if a consumer purchases a television from an online retailer and enters his name, shipping address, and other personal information at the site, the privacy policy for that company will disclose the choices. Clearly, when consumers input information at a website, they are aware of this fact and understand the choices with respect to such information. The widely accepted practice with respect to such information is the provision to the consumer of notice of the business’s information practices.

- ***“Context-based” advertisements should fall outside the scope of the definition of “behavioral advertising.”*** The definition of OBA should not encompass practices where information from the site — but not the consumer — is being used to deliver advertising. If there are no inferences being made about a consumer’s *behavior* online regarding “websites visited or content viewed” in order to deliver the advertisement, then this should fall outside the definition of “behavioral advertising.”

Thus, the scope of behavioral advertising should not include contextual advertising — those situations where the context of the website is used to determine the types of advertisements to be delivered or displayed. For example, if a website is aimed at golf enthusiasts and the site advertises golf resort vacations, this should not fall within the

scope of behavioral advertising merely because “advertising is delivered” based on the web page visited by all consumers. This is well within consumers’ reasonable expectation of the type of marketing that would occur. If the advertisement is placed based on the content of the web page being viewed or the type of web page, the advertisement would be delivered irrespective of what individual is viewing the web and the individual’s web-surfing habits. Such context-based advertising is no different than advertising in magazines, television shows, or newspapers, all of which are time-tested, successful models that have provided great benefit to consumers and businesses for decades (e.g., newspaper advertisement for furniture store placed in close proximity to article on remodeling).

- ***The phrase “the searches the consumer has conducted” should be eliminated from the OBA definition.*** This phrase encompasses too broad a range of activities, such as a site’s ability to deliver search results specifically requested by the user. As one example, based on the current definition of OBA and the current draft of the Proposed Principles, every site would have to either give an “opt-out” option, or obtain an “opt-in” (if “sensitive data” is at issue), before it could deliver search results *that the user had specifically requested*. E.g., Google, Yahoo, and any other search engine site, as well as other sites, such as individual retailer sites, would have to give an “opt-out” option if the user specifically input a search term (“automobiles” or “high definition television”) and hit “search” (or the site would have to obtain an “opt-in” in the circumstances identified). This result is nonsensical and would provide no consumer benefit. It would instead merely introduce a procedurally cumbersome step to have a consumer assent to something he/she already understands is occurring.

- ***Examples of overbreadth of current OBA definition.*** The following are examples of the overly broad range of situations to which the Proposed Principles would apply given the current definition of OBA. The definition should be modified so that examples (1) through (3) are excluded from the scope of the OBA definition, and consequently, excluded from the scope of the Proposed Principles.

(1) On-site advertising in which informational content on one site is tailored according to the search term(s) entered by the user and/or the content the user views *only on that single site*. No information (either PII or non-PII) is shared with any third party and no information (either PII or non-PII) is received from any third party. E.g., a person searches an electronics site for “television” and the site delivers results. The person then searches that same site for “dvd player” and the site delivers results for dvd players, and also includes results for televisions with built in dvd players.

(2) Ads delivered to any and every user viewing a particular website or content, such as an advertisement for a movie opening during the upcoming weekend is delivered on the homepage to everyone who visits an online publication that focuses on entertainment coverage.

(3) Paid advertisements delivered on a search engine as a result of a search conducted by the user. E.g., a search is conducted at google.com for “automobiles” and Google

delivers the “main” search results but also Google AdWords — i.e., the “sponsored links” at the top of and at the right hand side of the screen.

(4) “True” OBA in which an IP address visits site A, views content related to Baseball Team X; visits site B, views content related to City Y; and then a week later views content on site C, where an ad is delivered offering tickets for purchase when Baseball Team X will be playing in City Y.

With the necessary revisions described in this section, the remaining definition of OBA would focus on “true” OBA, such as the example given in number (4) just above.

V. Principle I Should Be Modified to Retain UDAP Principles But Eliminate the “Opt-Out” Concept

As currently written, Proposed Principle 1 embodies two distinct concepts: (1) clear and accurate disclosure of OBA practices (transparency); and (2) provision of an “opt-out” alternative from receiving OBA.

A. Transparency: OBA Practices Should be Clearly and Accurately Disclosed

We support the first concept captured in Principle 1: clear and accurate disclosure of OBA practices. This portion of the Proposed Principle furthers the interest in guarding against unfair and deceptive acts and practices. It also addresses the Commission’s concerns that OBA practices are “largely invisible and unknown to consumers” and that “consumers do not understand the role that data collection plays in OBA.”

B. The “Opt-Out” Portion Should be Eliminated

The second concept embodied in Proposed Principle 1 — the “opt-out” provision — advances no real privacy interests while substantially impairing internet usability, innovation, and customization to consumers’ detriment. It should be eliminated from any principles unless and until further serious study is undertaken on the possible loss and harmful effects to consumers, which are explained below.

1. Tracking Is Still Allowed

Under Principle 1 “consumers can choose whether or not to have their information collected for such purpose,” i.e., for the purpose of having targeted advertising delivered. Principle 1 thus on its face still *allows* online tracking, but if an “opt-out” is chosen, bans the *use* of such information *only for purposes of delivering targeted advertising*. By its own terms, Principle 1 does not bar collection of information and does not limit disclosure of information in any way (e.g., disclosure to third parties). It instead potentially bars a certain *use* of information (i.e., use of the information for advertising) by mandating an “opt-out” right from receiving OBA.

2. Information-Gathering Would Still Occur and Must Not Be Impaired

Even if information could *not* be *used* for advertising, in reality, information would still be gathered for many other practical purposes. Cookies and tracking are used for many purposes other than for OBA and facilitate provision of a vast array of benefits to consumers.

Uses of cookies and tracking other than for OBA include to facilitate online banking; to facilitate authentication and other security processes; to allow a website to recognize a user for other reasons, such as customized home pages on portals (e.g., Google), and retaining information on certain sites (e.g., Amazon); to facilitate research to improve navigability and usability of sites; and to determine the popularity of certain sites or site content among unique IP addresses. Further, a site might in fact need to track to be able to honor an “opt-out” from the receipt of OBA.

Following are examples of the benefits of information gathering practices, including practices connected with OBA and practices not directly connected with OBA:

- *Free content for consumers.* As the Commission has recognized, OBA facilitates free site content, such as no-charge newspaper sites.
- *Free services for consumers.* OBA also subsidizes services that allow a consumer to upload, share, and store videos and photographs at no cost. Similarly, it supports such online offerings as free e-mail, chat, video conferencing, and telephone service.
- *Reduced search and information costs.* In a similar vein, when an individual is interested in making a purchase or completing another kind of transaction, there are search and information costs, including the time spent in determining the types of products and services available and the prices of the various products and services. OBA facilitates lower search and information costs by subsidizing free search results and reducing search time. For example, when one searches on Google, “AdWords” often appear on the top and right hand side of the screen, and are provided in addition to the “main” Google search results. These “AdWords” subsidize the “main” search results, since the advertisers pay Google based on a formula. Both the “main” search results and the Google “AdWords” in the aggregate reduce search time and costs as compared with pre-internet days, greatly increasing consumer search efficiency.
- *Allowing new entrants in the marketplace, to the benefit of both businesses and consumers.* OBA creates cost efficiencies that directly result in allowing new entrants to the marketplace that otherwise would not be economically viable. OBA provides businesses with a more efficient and effective means of reaching consumers likely to be interested in their offerings. Such efficient and effective marketing enables new businesses to reach customers, thereby reducing costs to both businesses and consumers and improving competition. Such competition, in turn, results in significant corresponding consumer benefits in reduced prices and improved products.

- *Targeted advertising.* As the Commission has recognized, internet users may value targeted advertising.

- *Additional customized content.* In this ilk, users also value other customized content. Many internet users want a site to “know them” – e.g., remember their preferences, not be shown links in which they’ve repeatedly expressed no interest, and the like. Information-gathering helps to enable these functionalities.

- *Increased usability and navigability of sites.* Through research and analysis conducted by site operators and owners, internet information gathering facilitates increased usability and navigability of sites.

In sum, Proposed Principle 1 does not limit information-gathering, but rather restricts use of the information gathered with regard to uses for OBA. Further, any revision to Proposed Principle 1 must continue to allow this information-gathering in light of the wide ranging practical reasons that it must be collected (e.g., to aid with online security) and due to the numerous consumer benefits that result.

3. The Mandatory “Opt-Out” Would Not Further Any Consumer Privacy Interest

The proposed mandatory “opt-out” would not further any consumer privacy interest.

First, conspicuously absent from the Commission’s proposal is any distinction between the treatment of PII as compared with treatment of non-PII. The Commission’s principles apply to “data” and, thus, would appear to encompass both PII and non-PII. The identifying and non-identifying classification remains a critical distinction in any privacy framework and we do not believe that there is a “privacy” interest in non-PII. With regard to financial institutions, the transfer to third parties of PII, both for marketing and non-marketing purposes, is strictly regulated by law and corresponding regulations, including the GLBA and, with respect to certain types of PII, the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* This regulation includes the provision of notice and certain “opt-out” choices to consumers. Such choices are clear to consumers and provide a very effective means for consumers to limit transfers of personally identifiable information to third parties. Similarly, consumer choice concerning the transfer of PII to third parties for marketing purposes is a cornerstone of self-regulation in marketing and advertising and is incorporated into a number of existing self-regulatory frameworks, such as that of the Direct Marketing Association.

Second, as just explained in the preceding subsection, Proposed Principle 1 does not limit information-gathering, and any proposed revision must not impair this crucial need. Proposed Principle 1 also contains no limit on disclosure of information (e.g., it does not further any consumer privacy interest such as is embodied in the “public disclosure of private facts” tort). Proposed Principle 2 does contain such an implicit limitation, and as discussed below, we support such limitation in Proposed Principle 2.

Third, the Proposed Principles' undifferentiated "opt-out" does not further the traditional interest in barring unwanted "intrusion." In the internet realm, the user would still in fact receive advertising, and further, would simply lose the customized, pertinent advertising that OBA delivers.

Fourth, an "opt-out" does not advance any of the interests traditionally served by the "false light" and "misappropriation" theories. Instead, if anything, the Commission articulates a concern that OBA may portray the user in an *accurate* light.

4. The Proposed "Opt-Out" Would be Vague and Unworkable and, in Some Instances, Misleading

Information gathering may occur based on IP address. As a result, the proposed "opt-out" would be inaccurate and potentially both overbroad and incomplete.

The Principles seem to contemplate, and current technology allows, that an "opt-out" would be offered and exercised at the IP address level. However, unbeknownst to someone who may have thought he/she exercised an "opt-out," an "opt-out" might not "stick." And/or some "opt-outs" would be imposed on individuals who had not chosen an "opt-out". Either or both of these situations would undoubtedly occur where: an individual is using a different computer; the individual has moved his or her computer; the user buys a new computer; and/or there are multiple users of the same computer.

Any alternative idea to base "opt-outs" on individual sign-in is not viable. It would be unwieldy, impractical, and an impediment to anonymity to require each user to sign in to each website so that an "opt-out" choice could be presented.

5. The Remainder of the Principles Should Focus on Information Security and Limited Disclosure of PII

Revised Proposed Principle 1 addresses clear and accurate explanation of practices, and with substantial further work and revision indicated above, might cover appropriate consumer "opt-out" choices (e.g., modeled on the GLBA, an "opt-out" choice for transfer of PII to third parties for the marketing purposes of third parties could be given to authenticated consumers). Additional key consumer privacy protection concerns that may arise in connection with OBA that the remainder of the Proposed Principles should cover are: reasonable security for this information (as reflected in revisions to Principle 2), and limited disclosure (for legitimate business purposes only) of *personally identifiable information* (partially covered in Principle 2).

VI. Proposed Principles Regarding Data Security and Retention

Section 2 of the Commission's document sets forth two Proposed Principles that respectively address data security and data retention.

The Commission's Proposed Principle regarding data security states:

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 the company's business operations, the types of risks that a company faces, and the reasonable protections available to the company.

The Proposed Principle regarding data retention states:

Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

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, 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 are 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. 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.

In considering any revised principles, the Commission should consider whether it is appropriate to adopt standards already in place for financial institutions more broadly to apply to all entities that may have data used for OBA. Further, any revised principles should make clear that as for entities already covered by this existing law and regulation, that law and regulation applies to those entities, generally and also with regard to data used for OBA, rather than a data security portion of any revised principles.

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. Data retention issues should be considered under a reasonableness standard, rather than completely cabined by the narrower “legitimate business or law enforcement need” standard set forth in the Proposed Principle. Legitimate business and law enforcement needs are important characteristics of reasonableness, but there are also other factors that may be relevant.

VII. Proposed Principle 3 Is Aberrant, Would Encourage Anti-Consumer Practices, Should Be Inapplicable in Some Circumstances, and Must Be Substantially Modified.

A. Principle 3 Should be Limited to OBA

Proposed Principle 3 is broadly phrased and appears to address *all* handling or protection of consumer data in connection with notification of changes to privacy policies. The Commission is proposing Principles on “Online Behavioral Advertising.” All of the Proposed Principles, including Proposed Principle 3, should be limited to addressing OBA.

B. Principle 3 Should be Limited to PII

Principle 3 should also be limited to addressing notification of changes in privacy policy that touch on PII. Where only non-PII is at issue, no consumer privacy interest is at issue.

C. Principle 3 Should be Inapplicable when Existing Regimes Apply

Existing regimes, such as the GLBA and implementing regulations, already set forth requirements for notification of changes in privacy policy.¹ Layering Proposed Principle 3 on top of these existing requirements would create confusion among consumers and potentially conflicting standards. To the extent that existing regimes already address certain information potentially at issue with OBA (e.g., non-public personal information within the meaning of the GLBA), Principle 3 should be inapplicable.

D. “Affirmative Express Consent” Is a Departure from the Usual Standard, and also Creates Incentives Detrimental to Informed Consumer Choice

Proposed Principle 3 is also vague. In some portions it seems limited to suggesting that one must use data in accord with the privacy policy existing at the time that the data was collected. But other language appears to state that for *any* changes to a privacy policy, even for data collected on a “go forward” basis, a company would need to obtain “affirmative express consent” from consumers (*see*, e.g., Proposed Principle 3’s reference to a merger situation and a potential change in how companies collect data). This would

¹ 12 C.F.R. § 216.8.

be a substantial departure from current standards. For example, under the GLBA and implementing regulations,² a company can notify consumers of a change in collection, use, or sharing of data and there is no “affirmative express consent” requirement for such change to be effective.³

As written, Proposed Principle 3 also provides an incentive for companies to announce the least consumer-friendly privacy practices allowable. If a company announces a more stringent privacy practice than is legally required, under Proposed Principle 3, the company would have to get “affirmative express consent” from consumers before it could change its privacy practices. Such “affirmative express consent” would be extremely difficult to obtain from a majority of consumers. As a result, even if a company’s privacy practices went beyond legal requirements, companies would be loath to announce such practices, fearing that they would be binding themselves to such a practice indefinitely. This result would mean that consumers would have a difficult time comparing and shopping based on company’s actual privacy practices — an anti-consumer result.

VIII. Without Further Substantial Work and Revision, Principle 4 Should be Subsumed within Principle 1

Proposed Principle 4 seeks to introduce unique requirements for the use of “sensitive data” — a term that is not defined. Without definition, the principle is simply too vague. Indeed, if it were a statute, we believe that it would be invalid under the “void-for-vagueness” doctrine. The first step in any revision must be to define this term with specificity.

As one example of the havoc that the Proposed Principle’s vagueness could cause, some commentators to the Commission’s Town Hall suggested that “financial data” would be considered “sensitive data” with no limit that PII be involved. Under this conception, would the fact that an IP address originated a search for “debt consolidation” be considered “sensitive data”? If so, without the substantial revisions to the OBA definition laid out above in section IV, would this mean that a Google search for “five year auto loan” would require an “opt-in” so that Google could provide the main search results and also AdWords that underlay its business model? A financial institution site would have to obtain an “opt-in” before delivering content based on a customer search (the IP address initiates a search for “mortgage” and the site wishes to deliver mortgage

² 12 C.F.R. § 216.8.

³ The Gateway settlement, cited by the Commission in footnote 9, does not support a universal “affirmative express consent” standard to apply a change in a privacy policy. The Gateway document states that: “The policy also said that if Gateway Learning changed its policy, it would give consumers the chance to “opt-out” of having their information shared.” Among other complaints, the Commission charged that “Gateway Learning’s failure to notify consumers of the changes to its privacy policy and practices, *as promised in the original policy*, was a deceptive practice.” Last, the document inconclusively states that the settlement “prohibits it [Gateway] from applying future material changes to its privacy policy retroactively *without consumers’ consent*.” There is no explanation of whether “consumer consent” means notice and an opportunity to “opt-out” with the consumer not opting out within a reasonable time frame — as Gateway in any event had promised to do in its earlier privacy policy — or, obtaining “affirmative express consent” from consumers.

and home equity information)? This broad and ambiguous principle would necessitate unwieldy steps and processes without furthering any real privacy interest, as further explained below.

When and if the term “sensitive data” is defined, to the extent that the definition covers information already subject to existing law or self-regulatory regimes, that law and/or self-regulation should apply to such information, rather than layering on a potentially confusing additional set of requirements. For example, to the extent that the term “sensitive data” is meant to cover “financial data,” existing laws and regulations, including the GLBA and the Fair Credit Reporting Act, as well as existing self-regulatory regimes, already strictly dictate many requirements for financial data in which any privacy concerns are implicated (i.e., PII).

The only consumer privacy interest arguably unique to OBA based on “sensitive data” that the Commission articulated is a theory that, in a household where there are multiple users of a computer, OBA based on “sensitive data” might reveal confidential information about an individual to other members. First, the premise of this concern is dubious; advertising will still appear without OBA and user 2 does not know whether advertising is targeted or not. Second, any “opt-in” (or “opt-out”) would be an ineffective and potentially misleading “solution” to this concern, possibly providing the initial user with a false sense of security. Even without OBA, there are numerous ways in which information about user 1’s use of the computer can be discovered by user 2 such as temporary internet files, internet history logs, and browser caches.

The suggestion that use of “sensitive data” not be permitted at all, even with an “opt-in,” is nonsensical and extremely hostile to consumers and the wealth of free and fast information that the internet provides. Given the vagueness of the term “sensitive data,” the few examples given, and the lack of a definition for “advertising,” such a ban could mean (again, without substantial revision to the OBA definition) that even where someone explicitly asked for search results based on savings rates at certain dollar amounts deposited or mortgage rate based on purchase price and downpayment, the site would actually be prohibited from producing any such results that amount to “advertising.”

Without the further substantial work indicated above, Principle 1 (with the revisions indicated in section V above), should apply to both “sensitive data” and other data. Principle 4 furthers no additional privacy interest above and beyond the interests that Proposed Principles 1 and 2 and existing law and self-regulatory regimes already protect. Principle 4 should simply be eliminated (Principle 1 would thus cover all types of information, including “sensitive data,” as would Principle 2, and existing law and self-regulatory regimes would obviously remain intact).

IX. Section 5 of the Proposed Principles

Section 5 of the Proposed Principles seeks additional information about the potential uses of tracking data beyond behavioral advertising. Section 5 also specifically seeks comment on specified topics, e.g., any concerns around such secondary uses.

Section V.B.2 above sets forth additional purposes for which information gathered online is used for what the Commission calls “secondary uses” — i.e., for uses other than OBA. These purposes include to facilitate online banking; to facilitate authentication and other security processes; to allow a website to recognize a user for other reasons, such as to provide customized home pages on portals (e.g., Google), and to retain information on certain sites (e.g., Amazon); to facilitate research to improve navigability and usability of sites; and to determine the popularity of certain sites or site content among unique IP addresses.

None of these purposes raise any heightened concerns. Many of the uses involve only non-personally identifiable information, and further, because this section by its own terms asks about information that is used at least in part by OBA, consumers’ core privacy interests are protected by the Proposed Principles (with revisions suggested herein where applicable) — e.g., Proposed Principle 2 provides for data security.

If you have any questions or would like to discuss any of the issues raised herein, please do not hesitate to contact me at (415) 222-5798 or amy.b.lovell@wellsfargo.com

Very truly yours,

/s/ AMY B. LOVELL

Amy B. Lovell
Senior Counsel