



**NAI RESPONSE TO PUBLIC COMMENTS RECEIVED ON THE
2008 NAI PRINCIPLES DRAFT
16 December 2008**

In response to the Network Advertising Initiative's (NAI's) public call for comments on its draft 2008 NAI Principles document¹ through June 12, 2008, the NAI received numerous substantive and technical comments about various provisions of its draft proposal from a broad spectrum, including the online advertising industry, attorney community, privacy advocacy organizations, and a third-party auditing and accountability specialist. The NAI offers the following document as a summary of the comments received, in aggregate form, as well as a discussion of the NAI's response to that feedback.

In some instances the NAI agreed with concrete proposals put forward by commentators, adopting them explicitly in revisions to the NAI's provisional draft. In other cases, the NAI decided to retain the relevant provisions in the initial draft proposal, and to provide further explanation in this document. Finally, in numerous cases comments were received that were particularly helpful in suggesting criteria the NAI ought to use to apply the Code. Such "implementation" feedback was helpful to the NAI, and is acknowledged in this document, though frequently no corresponding modification to the Code was deemed necessary. This process culminated in a unanimous vote of the NAI to approve as final the 2008 NAI Principles Self Regulatory Code of Conduct, which reflects amendments discussed in this document.

The following discussion is structured topically. Where multiple comments were received on the same point, they have been consolidated and summarized for the sake of clarity. This document is ultimately intended to

¹ See 2008 NAI Principles: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising (Draft for Public Comment), *available at* http://networkadvertising.org/networks/principles_comments.asp, hereinafter ("Public Comment Draft").



promote greater transparency and understanding of the NAI's consensus-driven deliberative process.

1. SCOPE OF NAI MEMBERSHIP & CREATION OF IMPLEMENTATION GUIDELINES

Comments received:

Over the course of the past year, as well as during the open comment period, the NAI was urged to expand the scope of its membership beyond ad networks and to leverage the definitions of its Code more broadly. Although often this feedback was explicit, it also manifested implicitly in calls for extension of the NAI framework to newer forms of behavioral targeting implemented through data inspection by Internet Service Providers ("ISP BT").

Discussion:

As stated in comments to the Federal Trade Commission's December 2007 Proposed Behavioral Advertising Principles,² the NAI has been aware of calls to expand application of its Code beyond the third-party ad network context to a broader set of industry business models. Although the 2008 NAI Principles Draft for Public Comment did not explicitly propose to extend the Principles to other business models, through its public comment process the NAI sought specific input on whether the provisions of its Code could be adapted to other business models. The NAI attempted to determine whether extending the Code to other business models would necessitate differently-tailored implementations of some or all of the existing NAI Code standards

² Available at <http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf> (accessed 15 December 2008).



(particularly those that require provision of notice and choice about behavioral advertising services).

This fall, subsequent to Congressional hearings relating to the ISP BT model, the NAI announced its support for enhanced consumer protection through the provision of an opt-in mechanism in connection with this business model. In so doing, the NAI emphasized the technological distinctions between traditional Web-based advertising and other models that might involve substantially different approaches to data collection for behavioral advertising. The NAI reiterated its support for a sliding-scale framework that would afford increased levels of consumer choice based on the breadth, scope and nature of the data being collected and used for behavioral advertising.

In the final version of the 2008 Code, the NAI has continued this approach. The operative definition of third-party online behavioral advertising (“OBA”) within the Code continues to apply to the traditional models of Web-based behavioral advertising utilized by the bulk of the NAI membership.³ At the same time, while the full breadth of the NAI Code continues to apply to the ad network business model, the NAI also believes that its 2008 Code framework is extensible to similar business models, through the development of “implementation guidelines” specific to the particular model. By publishing an implementation guideline on a business practice covered by the 2008 Code framework, the NAI can provide consumers and businesses with clear explanations of how Code provisions apply to each business model and would be globally subject to the NAI self-regulatory framework.⁴ Additionally,

³ On this point, it is worth noting that the NAI’s membership and its corresponding collective ad serving marketshare continue to show strong growth. As of the date of the writing of this document, NAI membership has grown to 25 companies, with several more member applications pending. *See <http://networkadvertising.org/participating/>* (accessed 15 December 2008). Many current NAI members participate in the self-regulatory program and offer online advertising services diverse from traditional ad network products. Google Inc., Microsoft’s aQuantive division, Akamai, Yahoo! and its Blue Lithium product, and AOL’s Advertising.com division and Tacoda product are all active NAI Members.

⁴ Larger online companies that participate within the NAI maintain not only ad network products, but also other ad serving products that do not directly engage in OBA under the NAI Code. These other products may be appropriately addressed within an implementation guideline. Among the models already identified by the



although the 2008 Code in its present form does not address the issue of ISP BT, the NAI believes that the spirit of the consumer protection goals of the NAI's Self-Regulatory Code of Conduct might usefully inform future self-regulation of this business model.

In addition to providing the mechanism that will allow it to continue expansion of its membership to other appropriate business models over time, the NAI's implementation guideline approach is designed to leverage one of the unique core values of self-regulation: the ability to respond to changing circumstances and developments in technology. This vehicle will also allow the NAI to further refine and/or explain how it intends terminology within the Code to apply to a given situation, and to carry out the spirit of the consumer protections embedded in the NAI Code. The implementation guidelines for a particular business model, along with the underlying NAI Code, will be binding on participating companies.⁵ The NAI has identified certain subjects for implementation guidelines where it believes further explanation or refinement is needed to explain how the Code ought to apply to those models, or how the Code should treat those subjects. In certain cases these priority areas have been flagged in the Code text as well.⁶

2. FEEDBACK ON SECTION II TERMINOLOGY

Application of Terminology

Comment Received:

NAI for treatment in this manner are retargeting and ad platforms. *See* 2008 NAI Principles: The Network Advertising Initiative's Self Regulatory Code of Conduct, *available at* <http://www.networkadvertising.org> (hereinafter "2008 Code") *at* Section III.2(d) n.7.

⁵ 2008 Code Section IV.1(a) & (b).

⁶ *See, e.g.*, 2008 Code Sections II.8 n.4 (sensitive data); III.2(c) n.6 (reasonable efforts to enforce contracts); III.2(d) n. 7 (technology platforms). The NAI will also create an implementation guideline for retargeting practices.



One comment urged the NAI to explicitly clarify the point that that the terminology used in the NAI's 2008 draft for public comment is unique to the NAI's application of its own standards, and that alternate definitions for similar terminology in non-NAI contexts may remain entirely appropriate.

Discussion:

While the NAI believes that this point was at a minimum implied by language limiting Section II to "definitions . . . attributed to specific important concepts . . . in this document," it does see value in reinforcing this idea in light of various commercial activities or data uses that member companies may undertake that fall outside of the scope of application of the NAI Code, but which may be otherwise regulated or subject to other self-regulation that implicates common privacy terminology. The fact that a member company's practices fall outside the scope of activities intended to be governed by the NAI Principles does not imply that no privacy standards can or should apply to that NAI member's other business activities. Nor should the appropriate privacy standards for non-NAI governed activities necessarily be constrained in any way by the definitions in the NAI code.

Two excellent examples of this are found in the NAI Code references to "personal"⁷ and "sensitive"⁸ information, both discussed at greater length *infra*. Notwithstanding the NAI Code's delineation of what should at a minimum constitute personal or sensitive data in the online behavioral advertising context, numerous U.S. and global laws establish personal and sensitive data safeguards for different (or personal data transfer) contexts. NAI members

⁷ Public Comment Draft *at* Section II.5; 2008 Code *at* Section II.7.

⁸ Public Comment Draft *at* Section II.6 (Restricted and Sensitive Consumer Segments defined), and 2008 Code *at* Section II.8 (Sensitive Consumer Information defined).



operating as multinational businesses will continue to need to address applicable laws that may define privacy terminology in different ways, and the NAI Code does not purport to supersede application of those laws. The NAI's self-regulatory principles may, however, inform a better understanding of the types of data pertinent to online ad serving business models.

Action Taken:

The NAI will add the following clarifying language to the introductory paragraphs of Section II:

Although certain terms that appear in this Code are not unique to online behavioral advertising self-regulation, the NAI's application of this Code will be based on the specific meanings attributed to terms that appear in this Section. Alternate definitions for similar terminology in non-NAI contexts may remain appropriate for those contexts.⁹

Ad Delivery & Reporting¹⁰ and Multi-Site Advertising¹¹

Comments Received:

One comment urged the NAI to further outline self-regulation for members that not only engage in OBA but also for those that collect data through Ad Delivery & Reporting across multiple, unrelated websites. This is important, it was urged, because many consumers do not realize that information about the pages they are viewing may be collected and used to

⁹ 2008 Code *at* p. 4.

¹⁰ Public Comment Draft *at* Section II.2; 2008 Code *at* Section II.3.

¹¹ 2008 Code *at* Section II.2.



serve ads online. In addition, the data collected through such activities — e.g., page(s) visited, day and time of visit, IP address, and other identifiers — can reveal information about consumers generally and should be protected for the same reasons that the NAI deems OBA worthy of consumer privacy safeguards.

Accordingly, the comment suggests that the NAI impose its Notice and Security Principles upon any member that collects data through so-called “Multi-Site Advertising,” which could be defined as “Ad Delivery & Reporting across multiple web domains owned and operated by different entities.” In addition, to the extent a member engages in Multi-Site Advertising, it should further be subject to the Notice and Security requirements with respect to any Ad Delivery & Reporting activities on its own sites and services. As more entities join the NAI that collect data on their own sites and services for online advertising, it would make sense to capture these activities within the NAI Principles. Another commentator expressed concern that the NAI ought to capture practices that were not strictly “market segmentation,” but which nevertheless ought to enjoy certain Code level protections, even if they did not rise to the level of OBA. This could be achieved, one commentator suggested, by elevating all interest-based ad targeting however derived across domains to the status of OBA.

Another commentator underlined the fact that although the term “Ad Delivery and Reporting” is defined in the 2008 NAI Principles Draft for Public Comment to include “processes including but not limited to” certain provided examples, it was not clear to the commentator what other activities would fall within this definition. To delineate the scope of the definition, the commentator suggested that in addition to providing the specific examples, the NAI ought to specify that “Ad Delivery & Reporting” means “the logging of page views or the collection of other information about an individual consumer or computer for the purpose of delivering ads or providing advertising-related services.”



Finally, another commentator suggested that the NAI eliminate the “data that is not used to . . . locate an individual” phrase, given the NAI’s silence in the proposed code on classification of IP address. The suggestion is either to explicitly clarify how the NAI treats IP address or eliminate this phrase from the end part of the definition of Ad Delivery & Reporting so as to avoid muddling this issue.

Discussion:

Under the 2000 Principles, Ad Delivery and Reporting (on a single site) had always been subject to member notice requirements, whereas that traditionally defined as a “cross-website” behavioral activity (originally OPM) was subjected to more diverse sliding scale consumer protection standards, notably including pass-on notice requirements to publisher sites, appropriate consumer choices based on data type (opt-out, robust notice and opt-out, or opt-in), and in the case of PII use for OPM, standards such as reasonable access, security, reliability and constraints on onward transfer of data. These enhanced protections were justified by the privacy concerns relating to uses of behaviorally-related data for advertising purposes, even though these practices employ some of the same raw data used for Ad Delivery & Reporting. This approach has been practical and served the NAI well over time, because it helps the NAI to differentiate between common first-party data collection via cookies, web pixels, IP logs and the like – data that is required to load a web page and provide the content that a consumer’s computer directly asks to see – and the differing behaviorally-related advertising that third-party networks can enable using the same types of technology and data.

The 2008 NAI Code maintains this basic approach by focusing on the appropriate notice and choice regime for various *uses* of data, and assigning appropriate sliding scale safeguards depending on the relative sensitivity of data used for a given process. As such, the standard for Ad Delivery and



Reporting, which may use cookies or web beacons to enable the simple “counting” of ad clicks, for example, requires the provision of member notice just as it did in 2000.¹² While there is little privacy impact associated with this practice, the NAI believes that consumers ought to receive notice about these passive forms of data collection.

Just as in the 2000 Principles, the more robust data use associated with cross-domain behavioral advertising, described in the NAI’s definition of OBA,¹³ triggers enhanced requirements of pass-on notice and choice,¹⁴ and the other consumer safeguards contained in the Code.¹⁵ Notwithstanding the Code’s mission to focus primarily on the privacy impact of unique data uses, the fair information practices framework for consumer data is an important safeguard on secondary uses of that data. For this reason, the NAI has retained in its 2008 Code the requirements that data used by NAI members for covered practices should be subjected to security requirements¹⁶ and reliable sourcing,¹⁷ and, for the first time, has added data retention.¹⁸

In contrast to its approach in the 2000 Principles, the NAI has decided that such basic data protections ought not to be limited to the cross domain profiling-type activity, but should also apply for data collected in mere Ad Delivery and Reporting. Further, while the 2000 Code limited such protections to PII only, the NAI recognizes that since its members rely on non-PII for their activities, the same standards should apply equally to all data used for covered

¹² 2008 Code *at* Section III.2 (a).

¹³ 2008 Code *at* Section II.1.

¹⁴ 2008 Code *at* Sections III.2 (b) and III.3.

¹⁵ In fact, *every* provision in the 2008 NAI Code is applicable to OBA – the foundational self-regulatory privacy matter that the NAI Principles address.

¹⁶ 2008 Code *at* Section III.8.

¹⁷ 2008 Code *at* Section III.7.

¹⁸ 2008 Code *at* Section III.9, also *discussed infra* at p. 40-41.



purposes. The net effect of these updates is to extend the protections afforded Ad Delivery and Reporting beyond mere notice to include basic data safeguards (security, reliable sources and retention) that were not contemplated in 2000, for non-PII and PII alike.¹⁹

It is against this backdrop that the NAI further evaluated the commentator's proposal to add a new concept of "Multi-site Advertising" to its Code, and to determine how it should be treated within its sliding scale framework. The proposed addition of a "Multi-Site Advertising" category reflects the reality that there is in fact cross-domain Ad Delivery & Reporting that does not necessarily involve behaviorally-related advertising services, but which does involve comparable use of passive tracking tools like cookies, pixels and the like. Even where the privacy concerns associated with behaviorally-related advertising are not present, the NAI agrees that certain provisions of the Code ought to nevertheless be extended to Multi-Site Advertising, just as certain provisions (but not all) were extended in the 2008 revision to Ad Delivery & Reporting. By adding this third intermediate category of Multi-site Advertising within the definitions of its Code, the NAI will have a broader range of descriptors to draw upon to categorize emerging business models and will be better equipped to craft flexible implementation solutions. The upgraded requirements for Ad Delivery & Reporting apply to the new Multi-site Advertising category, which itself incorporates the same practices in a cross-domain context, with the notable addition of "pass-on notice" requirements for Multi-site Advertising. In the multi-domain context, notices should, therefore, appear on the sites that consumers are actually visiting. The NAI expects that its implementation guideline process will afford it an opportunity to further describe the types of practices that typically fall within the "Multi-site Advertising" self-regulatory scheme.

¹⁹ 2008 Code *at* Sections III.7-9. As in the 2000 Principles, 2008 Code Section III.6 (Access) remains unique to the authenticated PII circumstance.



The other pieces of feedback on the definition of Ad Delivery and Reporting were also explicitly adopted. The addition of “the logging of page views or the collection of other information about an individual consumer or browser for the purpose of delivering ads or providing advertising-related services,” reinforces within the Code that these activities may describe common ad delivery and reporting or multi-site advertising without necessarily implicating the more robust data uses associated with consumer interest segmentation that justifies higher privacy protections (those accorded to OBA in the 2008 Principles).

Furthermore, the suggestion to eliminate “data that is not used to . . . locate an individual” was adopted as well, given that this concept is better clarified in the Code’s updated definition of PII,²⁰ and of Sensitive Consumer Information.²¹ As suggested in those definitions, the precise location of an individual (such as can be ascertained through GPS-enabled devices) may well be of great use to enable highly-personalized targeted advertising, particularly in the mobile marketing realm. However, the privacy implications of precise geo-targeting are greater than those associated with more “approximated” traditional geo-targeting data points (such as may be garnered through IP-address lookup services or inferred through search terms, e.g.). Inferred or approximated data points about location (including assumptions made based on IP address) are insufficiently precise to be treated as PII under the 2008 NAI Principles, whereas real-time geo-targeting data tracking points are deemed not only personal information, but also are further elevated to the status of sensitive consumer information in the Code. In evaluating various forms of geo-targeting, the level of precision remains important in assessing the relative privacy implication of the data in question.

²⁰ 2008 Code *at* Section II.7.

²¹ 2008 Code *at* Section II.8.



Action taken:

Adopt definition of Multi-Site Advertising: "Multi-Site Advertising means Ad Delivery & Reporting across multiple web domains owned or operated by different entities."²²

Amend the definition of "Ad Delivery and Reporting" to read: Ad Delivery & Reporting is separate and distinct from OBA and means the logging of page views or the collection of other information about a browser for the purpose of delivering ads or providing advertising-related services, including but not limited to: providing a specific advertisement based on a particular type of browser or time of day; statistical reporting in connection with the activity on a website; and tracking the number of ads served on a particular day to a particular website.

As with OBA and Multi-Site Advertising, data used for Ad Delivery & Reporting purposes can include: type of browser, operating system, domain name, day and time of visit, and page(s) visited."²³

Adjust Section III requirements to reflect comparable protections for Ad Delivery and Reporting and Multi-Site Advertising.²⁴ Conform certain additional requirements for Multi-Site Advertising with those required of OBA.²⁵

Opt-Out of OBA²⁶

Comments received:

²² 2008 Code *at* Section II.2.

²³ 2008 Code *at* Section II.3.

²⁴ 2008 Code *at* Sections III.2 and III.7-9.

²⁵ 2008 Code *at* Sections III.2 and III.5-6.

²⁶ Public Comment Draft *at* Sections II.4 and III.3 (a) (i).



One comment urged the NAI to adjust the language of its proposed opt-out definition, to explicitly accommodate concepts such as “clarity,” “ease of use,” “accessibility,” and “simple explanations.” The commentator further urged that the choice ought to be “honored persistently until the consumer decides to alter the choice.” It is suggested that the cookie-based opt-out implementation of the NAI standard fails to ensure adequate “persistence of choice.”

Discussion:

The NAI invokes the opt-out terminology in various locations in its 2008 NAI Principles document. Substantively, the reference to the consumer choice mechanism first appears in Section III.2 (a) (v), where the NAI relies on a “clear and conspicuous” notice standard for an “easy to use procedure for exercising choice to Opt-out” with respect to OBA. In Section III.2 (b), the NAI goes on to require that members require any publisher with which they have contracted for OBA to “clearly and conspicuously post notice . . . on the website where data are collected for OBA purposes, that contains . . . a conspicuous link to the OBA choice mechanism.” Based on this language, the NAI is confident that the “clear and conspicuous” standard already codifies a focus on the “clarity, accessibility and simplicity” -- all relative concepts -- of the opt out. Further, the Code explicitly requires that the opt-out procedure be “easy to use.”

As such, the NAI believes that the Code adequately addresses the first portion of the commentator’s concern. Instead, this feedback is interpreted as broader concern that the implementation of this standard as it has been dispersed across thousands of websites could be more robust. Currently, the NAI has required that a link to its global opt-out page, or to the member’s own opt-out page, be available via the privacy policy of websites where data are collected for behavioral advertising services of members. This reflects the policy judgment that consumers are accustomed to seeking information



responsive to their privacy concerns at links labeled “privacy” on the homepage of various websites, where those websites communicate policies, practices and choices with respect to data collected actively on their website (via logon and registration pages, for example), and also passively (via cookies, pixels, and the like).

Within the context of a self-regulatory model in which network advertisers must implement a consistent consumer experience across literally hundreds of Web sites, the NAI continues to believe that notice through privacy policies remains the most effective and scalable approach to the issue of consumer choice. A clear and conspicuous, findable link on a homepage is an appropriate implementation of the “clear and conspicuous” standard under the NAI Code. The notion of “prominence” is already embedded in this definition, and changing the definition to include it does not modify the marketplace practice with respect to privacy policies.

The NAI’s approach to notice and choice does not, of course, preclude more robust approaches to consumer notice that might be adopted by Web page publishers and other participants in the online advertising ecosystem. In the past year, there has been considerable innovation in the broader marketplace in terms of more visible notices and consumer campaigns geared towards helping consumers learn about different types of behavioral advertising technologies. More innovation in the consumer notice sector should be encouraged, and rather than attempt to codify a particular approach to notice, the NAI Code leaves open the opportunity for other forms of enhanced notice.²⁷

With respect to the commentator’s second point, the notion of consumer control over the choice mechanism is also a double-edged sword that argues in opposite directions with respect to implementation. The behavioral advertising engaged in by NAI Members is still predominantly accomplished through use of

²⁷ See also further discussion of consumer education campaigns and enhanced notices, *infra* at pp. 27-28.



html cookies, which enjoy a high level of user control. Users can delete these cookies actively, or can passively ensure they are deleted by relying on default browser controls, downloadable software solutions, and the like. The cookies associated with behavioral advertising persist as long as the consumer decides to keep them, or at least as long as the consumer is aware of the consequences of changing browsers, systems, deleting their cookies, or of the default settings of either their browsers or of anti-spyware programs the consumer may employ. The consistency of this approach stands in contrast to browser-level configurations for consumer choice, as to which there may be considerable variation in the tools and steps necessary for the consumer to exercise similar choice.²⁸

The NAI agrees that to invoke granular choices the consumer must be given clear explanations of the circumstances under which they must invoke, renew or adjust their choices depending on their preferences. As such, in implementing the NAI notice (clear) and choice provisions (easy to use), the NAI will continue to require full disclosures of the circumstances under which opt-out choices must be renewed so long as a cookie-based opt-outs and privacy policies predominate in the marketplace and are implemented consistently in multiple browsers. Such explanations, it should be noted, do not *shorten* disclosures.

In sum, on these points, the NAI is reassured that its Code remains flexible enough to accommodate changes in the marketplace, as alternatives to cookies and alternatives to privacy policies that meet the NAI Code standards would be fully implementable going forward. However, the NAI cautions against mandating approaches that cannot be implemented across a broad number of websites, a broad number of browsers used to access the Internet, and, potentially, entirely new platforms of online activity. Such an approach

²⁸ This remains an area for continuing innovation, and the NAI looks forward to working with the various developers of browser technologies in existing and emerging platforms (mobile, e.g.).



would undermine the level and breadth of accountability already achieved and as reflected in broad-based use of privacy policy links, and html cookie controls.

Personally-Identifiable Information²⁹

Comments Received:

One commentator suggested that the "is used or intended to be used to identify, contact or locate" portion of this definition may not serve the NAI well. While acknowledging that members may not intend to use certain data for such purposes, it was argued that this is not a standard definition of personally-identifiable information used in other settings. Another commentator, however, explicitly noted this additional inclusion of data "intended to be used" and praised the NAI for its expansion on this point vis-à-vis the 2000 NAI Principles.

Another commentator argued that as drafted, it is unclear whether the definition of personally identifiable information was intended to include information that can be used to identify a particular individual only when combined with other data. Assuming that it was not, the commentator therefore recommended that the NAI clarify that personally identifiable information includes "information that, by itself, can be used to identify, contact, or locate a person, including name, address, telephone number or e-mail address."

One commentator expressed concern that the structure of the NAI's definition created an awkward result whereby widely-recognized PII such as name, address, telephone number or email address would only "count" as PII under the NAI code if it was actively used or intended to be used to identify, contact or locate someone. The commentator argued that these types of data

²⁹ Public Comment Draft, at Section II.5; 2008 Code at Section II.7.



should instead always be treated as PII whenever they are collected, regardless of their intended use. Another commentator agreed with the proposition that certain data ought to be considered PII regardless of intent.

Finally one commentator separately recommended that the NAI support the de-identification of personally identifiable information as an industry best practice. Consumers, it was argued, are best served when upfront steps are taken to ensure that information that can be used to personally and directly identify them is separated from information collected through multi-site or behavioral advertising.

Discussion:

The NAI acknowledges that its modification of the definition of PII in its Code to include data intended to be used as if it were PII, whether possible only in combination with other data or not, is specific to the context of online behavioral advertising that the NAI Code endeavors to self-regulate. That this definition of PII does not exactly match definitions used in other contexts should not be problematic, as the same may be said for much of the terminology used in the NAI code. As noted previously, the terminology used in the Code is intended to be unique to this Code, and other definitions in other contexts remain entirely appropriate.

Further, this standard acknowledges that information that is not PII in one context may be PII in another, and should receive higher protection in the latter context. Similarly, the "intended" standard also reflects the reality that NAI Members in many instances take express steps to prevent the non-PII data they collect for advertising purposes from becoming identifiable.³⁰ The NAI believes that its Code should continue to promote such efforts. By

³⁰ Indeed, in many cases companies affirmatively intend not to identify individuals, and achieve this result through de-identification technologies such as one-way encryption. Use of de-identification processes is one factor that can inform a determination as to whether data used for OBA is non-PII or PII.



imposing higher obligations for uses of PII, the NAI Code creates strong incentives to use only non-PII for behavioral marketing purposes. In the instance where a Web site operator may want to offer personalized experiences to its authenticated users, the use of de-identification technologies can help ensure that alternate use of data for behaviorally-related advertising remains non-personally identifiable.³¹

Having clarified this point, it should be evident that the NAI did not intend this definition to be limited only to data that by itself may be identifiable, but also to contemplate merged data and other data uses that are intended to identify an individual. The focus is not on what “can” be done, as is the focus of the discussion relating to data security, *see infra*, but instead on what “is” or “is intended” to be done. The actual use or intended use should trigger appropriate consumer choice levels – as structured in the Code. What “can” be done with certain data should, in the NAI’s view, inform the reasonable security put around that data. This concept is addressed in the NAI’s updated security standard.³²

However, the NAI agrees that an unintended consequence of its drafting was the possible suggestion that certain data listed such as name, address, etc. would not be considered PII unless the actual use or intended use conformed to that status. This was admittedly not the intention behind this enumeration of examples. Instead, the NAI agrees that certain data, even beyond what was enumerated in the draft, should always “count” as PII regardless of use or intent.

Action Taken:

³¹ Alternate approaches that fail to recognize the value of the non-PII anonymous user experience, by calling for opt-in for all data types, undermine the layer of consumer protection that de-identification technologies provide.

³² 2008 Code *at* Section III.8.



Amend the proposed principle to explicitly confirm the status of certain data:

“PII includes name, address, telephone number, email address, financial account number, government-issued identifier, and any other data used or intended to be used to identify, contact or precisely³³ locate a person.”³⁴

Restricted & Sensitive Consumer Segments³⁵

Comments Received:

Multiple commentators felt that creation of two terms – restricted – and sensitive—to describe the same categories of consumer segments was confusing and muddled. While acknowledging the different policy bases for regulating use of non-PII for sensitive categories and PII for sensitive categories, these commentators suggested that for NAI purposes the categories are the things that are “sensitive,” notwithstanding the type of data used. If the NAI wished to maintain different choice levels for non-PII use in sensitive categories and PII use in sensitive categories, it was argued, it could accomplish this in a clearer way by stating this in the Choice or Use Limitation sections, relying on a simpler definition of Sensitive Consumer Segments.

Another commentator suggested that the NAI not limit its treatment of sensitive information to practices involving the use of “consumer segments.” Second, the commentator urged the NAI to provide clearer and more definitive guidance on what information is sensitive. For example, one commentator

³³ See also *supra* pp. 11-12 for a discussion of the treatment of IP address as non-PII under the 2008 Code.

³⁴ 2008 Code *at* Section II.7.

³⁵ Public Comment Draft *at* Section II.6; 2008 Code *at* Section II.8.



urged the NAI to focus on specific sets of data types it considers sensitive, however used for OBA.

Another commentator urged the NAI to conduct consumer research to determine the categories of information that is considered sensitive by most individuals, as it was not persuaded that the listing selected by the NAI was sufficiently definitive. In the end, it was argued, the NAI's research should focus on determining the potential harm to consumers if certain types of data are used for behavioral advertising. In any event, several commentators agreed that the NAI's proposed draft list of sensitive consumers segments were too confusing or imprecise to be broadly implemented in an objective way at this stage.

Finally, another commentator indicated that the NAI should reconsider its proposal to obligate members to obtain opt-in consent before using "restricted consumer segments" — i.e., non-personally identifiable "sensitive" information — for OBA. In essence, the commentator suggested that any opt-in protections be limited to use of PII, and that even in the PII context sensitive categories should be treated as any other PII use in the Code, i.e. allowable with opt-in choice, as opposed to an outright prohibition. Any prohibition on the use of such information, it was argued, could harm consumers by preventing members from serving those consumers who believe they could benefit from more relevant advertising related to sensitive areas, like health. For example, a consumer with a particular health problem may want to learn about offers on particular treatments for that problem. Consumers should be afforded the opportunity to make these decisions, and members should be given the flexibility to provide consumers with this information. While the commentator stated that it appreciates the privacy implications of using sensitive personally identifiable information for OBA, it urged that these concerns can be appropriately addressed by requiring members to obtain prior affirmative consent from consumers. Such an opt-in approach provides members with the flexibility needed to serve consumers'



interests while giving consumers control over whether sensitive information about them is used for this purpose.

Discussion:

As discussed in the proposed Principles Addendum A, the NAI believes strongly that valid privacy concerns are raised by the prospect of using certain information as the basis for behaviorally-targeted online advertising campaigns. Further, the NAI acknowledges comparable privacy concerns apply to the use of any consumer data in sensitive market segmentation.

Given that consumer privacy expectations vary greatly by person, culture and context, any attempt to label consumer data as sensitive is an inherently difficult and subjective undertaking.³⁶ It is clear that what makes one consumer personally uncomfortable may bear little relation to the privacy expectations of another consumer. Nevertheless, the online behavioral advertising marketplace, the NAI has argued, would benefit from enhanced clarification as to how OBA should work in order to remain compatible with expectations when sensitive consumer data and market segments are involved. This effort is critical to maintaining consumer trust in marketing undertaken by third parties that do not have a direct relationship to consumers.

The NAI sees value in accepting feedback that will help clarify the document to consumers and press to the extent feasible. Many of the distinctions made in the NAI's draft Code were, admittedly, quite specific. This therefore required the reader to navigate complex concepts and terms in order to correctly apply provisions. In light of feedback on this point, the NAI agrees that eliminating the term "restricted" will not substantially impair a business' understanding of the appropriate choice levels set by the Code for sensitive data.



Additionally, the NAI accepts the feedback that its “market segments” approach was perhaps too subjective a standard to be helpful within an industry Code at this time. The NAI remains interested in continuing work on this important concept, and welcomes additional input from stakeholders on the right ways to identify categories that ought not to be used for behavioral marketing purposes. The use of “traditional” PII or non-PII for certain types of “sensitive segmentation” remains a concern of the NAI, and as such a framework that recognizes certain segmentation as sensitive will be revisited in an implementation guideline on this point. Following the suggestion of commentators, however, the proposed framework will replace the definition of “sensitive consumer characteristics” with a definition of data that will always be deemed “sensitive” and will as such require “opt-in consent” regardless of the type of segmentation used. The benefit of such an approach is that it will be better understood by the privacy community than the concept of behavioral segments originally proposed. However, further refinement of the meaning of “precise health information” in an implementation guideline, particularly, will still be required to differentiate between commonplace non-sensitive health-related matters and those that are truly sensitive.³⁷

Finally, the NAI acknowledges the feedback that the highest reasonable standard that ought to be imposed on industries that provide positive services for consumers is that afforded by the NAI’s Opt-in standard.³⁸ The NAI agrees that there is no real benefit to consumers to prohibit outright the provision of any sensitive-data personalized advertising services that a consumer may deem beneficial. For those circumstances, express affirmative consent (the NAI opt-in standard) is adequate to protect consumer privacy. The NAI disagrees, however, with the blanket proposition that non-PII used in a sensitive context

³⁷ To achieve an appropriate reflection of distinctions between health conditions, the NAI intends to engage in further discussion and has already begun affirmative outreach with stakeholders from the health industry, privacy specialists and consumer research groups to better understand how the NAI ought to evaluate OBA marketing on health conditions, or use of precise data.

³⁸ 2008 Code *at* Section II.4.



will never raise privacy concerns superior to any other non-PII use for OBA. While most sensitive data under the new Code framework will also be PII, some of it may not, and the opt-out standard for non-PII use and prospective PII use alike is only appropriate under the NAI code where no sensitive data is implicated. A contrary result would render the sensitive information category functionally meaningless. As such, the NAI will retain the Opt-in standard for any data use for OBA, Multi-site Advertising or Ad Delivery & Reporting that meets the Code's amended definition, even where data being used is otherwise classified as non-PII. The resulting provision of a single standard for all sensitive consumer information use will promote greater clarity for businesses while ensuring that the highest standard of consumer choice applies in the "sensitive" context.

Action Taken:

For the sake of greater clarity the NAI will refer merely to "sensitive consumer information" to be amended accordingly, as suggested by commentators. In some cases sensitive consumer information may also be PII, but it need not be. It adopts specific data types as sensitive, as suggested by commentators, including Social Security Numbers or other Government-issued identifiers; Insurance plan numbers; Financial account numbers; Information that describes the precise real-time geographic location of an individual derived through location-based services such as through GPS-enabled devices; and Precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history.³⁹

³⁹ The NAI places significant emphasis on the use of the term "precise" in its sensitive health data definition. The Code does not establish an opt-in standard for all health-related advertising, or use of data from health-themed sites. There are, as articulated in the NAI draft proposal, certain medical issues that may be deemed sensitive, and others that are not. In connection with the formulation of an implementation guideline, the NAI will look to existing industry standards and applicable law (for example the California



The subjective “sensitive consumer segments” categories will be withdrawn from the final Code but may be revisited in an implementation guideline to further develop the notion of sensitive data use in the behavioral advertising context. The Section III requirements will also be updated accordingly to acknowledge the conforming modifications to the choice and use limitations, in light of the above discussion.

Marketing Purposes⁴⁰

Comment:

One commentator urged the NAI to elevate this term to the definitions section, given its importance, and to clarify whether the NAI interprets this definition as broad enough to embrace “differential pricing.” If so, the commentator urged the NAI specifically call out this practice and lengthen disclosures systematically across all notices to reflect this reality.

Discussion

The NAI accepts this piece of structural feedback as helpful, and has indeed elevated the already-broad definition of marketing practices to Section II of the final Principles. The NAI intends this provision to be construed broadly, so as to account for a variety of marketing practices, including those innovative data practices that have not yet been developed. As such, differential pricing certainly could fall under this definition, although it is already subject to existing marketing laws. However, apart from other types of

data breach statute, which focuses its definition of medical information on data gathered in the context of the physician-patient relationship).

⁴⁰ 2008 Code *at* Section II.9.



data used for behavioral advertising, it is entirely unclear why only one potential behavioral marketing sub-practice would be called out separately from a requirement that already exists: namely, to disclose how behavioral targeting data will be “used.”⁴¹ At the Code level, the NAI believes that adding rigidity and further specificity to the form and content of disclosures would not be a prudent course in light of calls to shorten, simplify and make easier-to-understand those very disclosures. This is particularly so where the Code already requires a disclosure of data uses – the implementation of that requirement is subject to case by case analysis, and differential pricing is not widely considered a “common disclosure” separate from “behavioral advertising” type data use disclosures.

Instead, the NAI intends this new Code enhancement⁴² to function as a true use limitation provision, one that prohibits secondary uses of behavioral segments for non-marketing purposes. The NAI received feedback from some commentators fearing that harmless marketing segments might otherwise “fall into the wrong hands,” or be misused for harmful secondary purposes such as identity theft or adverse insurance determinations. The NAI believes that this provision explicitly addresses that concern within the self-regulatory framework. Further protection is offered by the NAI’s security standard, which applies to all “data” used for covered practices. These two provisions, -- the marketing use limitation on behavioral segments and the reasonable security for all data -- operating in tandem, should reassure the public that the Code has explicitly addressed this concern.

Action Taken:

⁴¹ 2008 Code at Section III.2 (a) (iii).

⁴² Note that the 2000 NAI Principles never contemplated such a limitation on secondary use of behavioral advertising data.



Add definition to Section II: “Marketing Purposes includes any activity undertaken to collect, aggregate, analyze, maintain, update, or sell information in order to tailor content or services that allows or induces consumers to take action to purchase, rent, or exchange products, property or services, to solicit a charitable donation, to utilize market research or market surveys, or to provide verification services to marketers. Certain non-marketing uses of OBA segments may already be restricted by law.”⁴³

3. FEEDBACK ON SECTION III: REQUIREMENTS FOR NAI MEMBERS

Transparency⁴⁴ and Consumer Awareness

Comments Received:

One commentator indicated that Section III.1 (b)’s requirement that members “use best efforts” to inform consumers about behavioral advertising is vague, and it is unclear how the NAI would enforce it.

Another commentator praised the NAI for allowing this commitment to figure so prominently in the Code, and emphasized that transparency is an exceedingly important goal in an area where few consumers have direct relationship with third party ad networks. To help consumers understand how to make NAI members’ opt-out mechanisms work, the NAI was urged to provide detailed explanations of browser configuration issues on its Web site. Although the NAI already provides links to instructions for how consumers can enable third-party cookies in their browsers, it was argued, a listing of other configuration issues and instructions for how to fix them should be added to promote transparency. Although the NAI Web site is consumer-facing and the

⁴³ 2008 Code *at* Section II.9.

⁴⁴ Public Comment Draft *at* Sections III.1 (a) & (b); 2008 Code *at* Sections III.1 (a) & (b).



principles themselves are directed at network advertisers, it was also suggested that the Principles should be linked directly from the NAI Web site.

Discussion:

With respect to the first point, the NAI agrees that businesses implementation efforts should be subject to an equivalent standard for all provisions. The appropriate standard is one of "reasonableness."⁴⁵

On consumer awareness generally, the feedback relating to this provision is well-taken by the NAI, and acknowledged as helpful with respect to implementation of the proposed provision. It is also related to the question of notice. Website updates are indeed envisioned as part of the updated NAI Principles 2008 framework, and this feedback will be accounted for in that implementation. Moreover, NAI members like Yahoo!, Google and AOL have already begun to experiment with enhanced forms of notice and education designed to capture consumers' attention beyond and outside of privacy policies. In some cases this may help drive more consumers to privacy policies and the ability to opt-out.

In its comments to the FTC earlier this year, Yahoo! outlined one new approach to contextual notice in advertisements, which can be effectively deployed in certain contexts, as well as its chef-themed public service announcement about ad customization.⁴⁶ In the case of Google, there have been innovations with respect to video notice about behavioral advertising,⁴⁷ leveraging YouTube-style information videos akin to those entertained by the

⁴⁵ See 2008 Code at Sections III.1 (b), III.3(c) & (d), III.6, III.7, III.8.

⁴⁶ See "Ebay adchoice contextual notice sample," available at <http://www.ftc.gov/os/comments/behavioraladprinciples/080411yahooappendices.pdf> (accessed 15 December 2008).

⁴⁷ See, e.g., Google consumer privacy videos, available at <http://ie.youtube.com/user/googleprivacy> (accessed 15 December 2008).



FTC at its Town Hall.⁴⁸ These are widely available and readily accessible to consumers, and do not require reference to written disclosures. In the case of AOL and Tacoda, a virtual penguin has endeavored to guide consumers to better understand what behavioral advertising is, where it happens, and what choices consumers have about it.⁴⁹ These are laudable forms of macro notice about behavioral advertising outside the privacy policy. The NAI fully supports its members' continued experimentation with enhanced consumer outreach on behavioral advertising and sees further development in this arena as a promising adjunct to website-based notices that appear at the point of data collection.

In short, the NAI website, improvements and simplification of website notices, and online campaigns serve collectively as transparency tools that reinforce the implementation of the NAI Principles consumer framework, and of the "notice" that consumers can get about behavioral advertising.

Action Taken:

Clarify "reasonable" standard as common throughout the Code, in Sections III.1 (b); III.2 (c) & (d); III.6; III.7; III.8.

Notice⁵⁰

Comments received:

⁴⁸ See FTC Town Hall video contest submissions on "cookies," available at <http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml> (accessed 15 December 2008).

⁴⁹ See AOL consumer video on behavioral advertising, available at <http://corp.aol.com/o/mr-penguin/> (accessed 15 December 2008).

⁵⁰2008 Code at Section III.2.



Echoing some of the discussion related to the visibility of the opt-out tool,⁵¹ one commentator suggested that the “clear and conspicuous” standard should be replaced with explicit focus on “clear, concise, consumer-friendly and prominent” statements.

Another commentator acknowledged the utility of the “opt-out status” reading on the NAI’s consumer website, and suggested that all members be required to replicate it on the member’s own website.

One commentator expressed concern that the NAI’s pass-on notice requirement allowance for a member to “ensure, as applicable,” that notice appear on a website could be misconstrued to justify not providing the notice if the member deemed the requirement “inapplicable.” The commentator also sought clarity on the application of the pass-on notice requirement in the absence of a contract. The commentator insisted that the greatest value is achieved by requiring a link to the NAI global opt-out, rather than just the member’s own opt out. This will ensure that consumers can readily learn about other NAI members that may be using cookies to personalize advertising online to the consumer. Finally, the NAI was urged to explicitly acknowledge that browser-level notices could be adequate to satisfy its notice standards, as an alternative to privacy policy notices.

Discussion:

The NAI’s position on the clear and conspicuous standard is addressed earlier in this document.⁵² The remainder of the comments received on this Section are well taken, although they do not all require Code adjustments to adopt them as propositions. Although it was intended to acknowledge that circumstances may require alternate notice delivery mechanisms, the NAI

⁵¹See discussion, *supra* at pp. 13-16.

⁵² See discussion, *supra* at pp 13-14.



agrees with the comment that notice should always be applicable, and agrees to strike the apparently constraining clause “as applicable.”

The comments about the availability of the global opt-out page on the NAI website and access to the “status” button can be addressed together, by requiring a link to the global opt-out page as suggested by adding the clause “and/or a conspicuous link to the opt-out page on the NAI’s consumer website” to Section III.2(b)(iv). Finally, the NAI agrees that notice through a web browser, if sufficient to meet the Code’s clear and conspicuous and “ease of use’ standard, could be one implementation that satisfies the notice requirement. There is no apparent need to list within the Code, however, this fact. An implementation guideline, as necessary, would be preferred to clarify how a member seeking to implement such a browser-based notice would do so in conformity with the Code, should such a practice become prevalent.

Action Taken:

Remove “as applicable” from Section III.2 (b) to now read: “Each member directly engaging in OBA and/or b) Multi-Site Advertising shall require that a website with which it contracts for OBA and/or Multi-Site Advertising services shall clearly and conspicuously post notice—or ensure, that such notice be made available on the website where data are collected for OBA and/or Multi-Site Advertising purposes—that contains . . .”

Adjust Section III.2. (b)(iv) to read “A conspicuous link to the OBA choice mechanism (e.g., iv. Opt out link) provided by the NAI member, and/or a conspicuous link to the opt-out page on the NAI’s consumer website.”

Choice⁵³

Comments:

⁵³ 2008 Code *at* Section III.3.



Much of the feedback received on this Section related to concerns that outright bans on data use were unnecessary, and that the highest standard that ought to be applied to redress privacy concerns is the express affirmative consent standard.

Other comments reiterated the criticism that cookie-based opt-outs were poor implementations of the choice principle, but did not provide concrete proposals that could be considered as viable alternatives. One commentator outlined how a “browser-based” opt-out might work, but apart from this suggestion did not explain how a self-regulatory organization of network advertisers could ensure that all the browsers used by consumers could effectuate a behavioral advertising opt-out request in a comparable manner and scale as to that provided by use of http cookies.

Additionally, a technical comment was received that pointed out that not only mere “provision” of choice mechanism be required, but also that they must work and be honored.

Discussion:

Prohibitions contained in the draft Code appeared in only two places: PII used with Sensitive Consumer Segments,⁵⁴ and use of Children’s segments.⁵⁵ Ultimately, the basis for the two prohibitions was somewhat distinct. In the former case, the prohibition was contemplated as an attempt to codify what many members already urged was common practice: to avoid or prohibit the sale for targeting against certain sensitive segments. This practice emerged as a direct reflection of the consumer trust proposition – by voluntarily agreeing to limit practices in this way, NAI members sought to

⁵⁴ Public Comment Draft *at* Section III.4 (b).

⁵⁵ Public Comment Draft *at* Section III.4 (a).



reinforce consumers' confidence that they can trust engaging with NAI members in the online medium. However, the NAI ultimately agrees that this premise is achieved through comparable measure to limit such data use to only those circumstances where consumers expressly consent to such data use. This will functionally limit the scope of the practices to only those circumstances where the direct consumer benefit of such sensitive targeting is sought by the consumer herself, and should engender a comparable level of consumer trust.

With respect to opt-out mechanism, as stated in its Comments to the FTC Proposed Principles,⁵⁶ notwithstanding the fact that the NAI has adopted one common implementation for its members' opt-out that is cookie-based, it is important to note that the draft 2008 Principles never mandated cookie-based opt-outs. Instead, the Code spoke of "opt-out" without specifying or requiring a specific technological response. The NAI believes this approach to its Code is still sound. The NAI wants the Code to remain flexible enough to allow other non-cookie based opt-outs to be compliant.

However, because traditional cookies provide such high levels of transparency and consumer controls through web browsers, and consumers' ability to manage/delete them is quite well-developed, the NAI feels strongly that any alternatives to traditional cookies emerging in the marketplace as choice mechanisms must afford consumers comparable levels of transparency and user control. By failing to require or codify cookie-based alternatives to it, the NAI recognizes that emerging browser-based technologies may achieve significant innovations in consumer choice. The NAI will continue to scrutinize its Members' choice implementations to ensure that appropriate transparency and controls are in place to effectuate the opt-out consistent with the Code.

⁵⁶ See NAI Comments, *supra* note 2 at 25-26.



Furthermore, while browser-based opt-outs may hold promise, until all browser manufacturers adopt them to the same level that cookies are recognized, and until all NAI members are able to commonly implement them as they have been able to commonly implement cookie-based opt-out, the “global opt-out” function that is a core benefit to consumers of the NAI’s self-regulatory structure would be compromised. Any alternatives to the present implementation on the NAI website must seek to be non-partisan with respect to type of browser – it cannot be limited to only one browser implementation, however ubiquitous. Second, it must be accessible to a comparable range of market players that wish to join the NAI. The NAI members must provide a functioning opt-out mechanism that they can honor. If, rather than cookie-based mechanisms, consumer choice were achievable through specific browser settings that users can control, this would be a positive result for consumers. Over time, the NAI and its members may furnish cookie-based global opt-outs that will be honored *and* continue to work with browser providers to tailor innovation that reflects the fundamental policy objectives of the NAI Code.

It goes without saying that ongoing testing and information about how to work with NAI opt-out cookies is important to the vitality of the program, and that the NAI Code is intended to require not only the “provision” of an opt-out mechanism, but one that works subject to consistent testing on various platforms, and that can and will be honored by all NAI members. With respect to the technical comment then, the NAI agrees that reference to “provision” of a choice mechanism is not enough – the mechanism must work and be honored as well.

Action taken:

Amend Section III.3 (a) to clarify that “provide and honor” is the standard for all subsections relating to provision of a choice.



Children's segments⁵⁷

Comments Received:

Multiple comments urged the NAI to reconsider its proposed blanket prohibition on members' creation of a behavioral advertising segment specifically targeting children for a variety of reasons.

First, one comment reflected concern that such a prohibition, even if limited to the creation of an OBA segment, would likely be misconstrued as a statement by the NAI that it believes advertising is harmful to kids. Ongoing routine collection of non-PII on child-oriented websites might also raise a question as to whether such data, when used for OBA purposes, could taint a marketing segment and render it one "targeting children under the age of 13."

Another comment echoed the sentiment that prohibitions should only be invoked when a particular harm is tied to the practice in question. In this instance, the commentator urged the NAI to conduct research on this topic and to target its Principle only to a harm that has been identified.

Multiple comments pointed out that targeting of children's ads should actually be considered beneficial. Advertising tailored to children may be more appropriate for children than generic untargeted advertising that the child might otherwise view online. One of the consequences in failing to target ads to children is the possibility that they might see something that is not meant for them. The Children's Advertising Review Unit (CARU) self-regulatory guidelines describes disclosures and ad selection approaches adapted to children's advertising, and ought to be accounted for in the NAI's approach to the subject. In essence, one unintended consequence of the prohibition might

⁵⁷ 2008 Code Section III.4 (a) and n. 8.



be that children would be served a higher proportion of ads for products that are not for children.

Finally, one comment urged the NAI to clarify the intended scope of its prohibition with respect to various questions:

- Would this provision prevent children from seeing online ads?
- Would it be permissible to create a marketing segment of interest to adults and children alike (e.g. action figure enthusiast, cartoon enthusiast, Lego enthusiast, Dora the Explorer enthusiast?)
- Will this impact contextual serving of child-oriented ads on COPPA-governed sites?
- If a member obtained verifiable parental consent to tailoring of ads, would this be a permissible exception to the prohibition?

Discussion:

The NAI agrees that treatment of children is different than other potentially “sensitive” topics, due in part to the existence of both regulatory and self-regulatory safeguards around children’s advertising in general. It is for this reason that the NAI decided to treat the matter separately from its proposed “restricted and sensitive consumer segments” Principles.

The NAI also agrees, and wishes to make explicit, that a prohibition is not to be construed as a statement that advertising is harmful to children. This prohibition was carefully drafted so as only to apply to the specific practice of OBA, which implicates non-contextual ad targeting, and in no way impacts the serving of contextual ads on child-oriented websites. The NAI acknowledges that children’s advertising guidelines such as required by CARU remain appropriate ad-tailoring criteria for online contextual advertising on COPPA-governed sites. Many NAI members enable contextual ad serving for child-oriented products marketers, and include COPPA-governed websites within



tailored ad-networks. Neither ongoing service is intended to be impacted by the prohibition.

The NAI also agrees that marketers of products of interest to adults and children alike ought to be able to benefit from OBA services offered by NAI members. The permissibility of an NAI member offering such services to marketers of such products under the new standard would depend, therefore, on the manner in which the marketing segment would be created and labeled. The standard covers marketing segments *specifically* targeting children under the age of 13. This prohibition is designed to reassure the public that any perceived identification of children by a marketing segment (in the case of PII or non-PII alike) would not occur in the absence of parental consent. Any non-PII market segment called “children” would likely to be perceived as identifying children, even if it does not identify any one child specifically, and this perception would have an adverse impact on consumer trust of the OBA industry.

The unique challenges associated with obtaining consent formed the basis of the NAI’s decision to adopt both a non-PII and PII prohibition of the creation of children’s segments in connection with OBA. Children cannot themselves consent to such practices even in the case of PII-based targeting, nor should they be expected to exercise opt-out choice based upon clear and conspicuous disclosures. The NAI agrees, however, that if verifiable parental consent to engage in PII-based OBA of that parent’s child can be obtained, this prohibition ought not to apply.

Action Taken:

Having discussed these points, the NAI has determined in light of comments to retain proposed § III.4 (a), with the addition of a concluding limiting clause “, without verifiable parental consent.” In addition, the NAI will add two clarifying notes. FN 8 will be expanded to acknowledge that NAI



members relying on children’s PII should refer to CARU guidelines for contextual ad selection, which remains otherwise unaffected by these Principles. Where children’s PII can be used to tailor ads through non-contextual OBA services, the prohibition of § III.4 (a) shall not apply where the member can obtain verifiable parental consent, as defined by COPPA.

Transfer and Service Restrictions⁵⁸

Comments Received:

One commentator identified a point of confusion in the drafting of Section III.5 (b), which referred to “third parties” and “third-party publisher or advertiser” as if a distinction was intended. The commentator suggested simplifying the phrase to apply to “third parties” consistently.

Discussion:

The NAI agrees that the proposed adjustment would better reflect the fact that this provision could apply any third party regardless of business model, although publisher and advertiser contracts predominate at this time.

Action taken:

The text of Section III.5(b) is amended to read: “Members shall contractually require that any third parties to which b) they provide non-aggregate non-PII, to be merged with PII data possessed by that third party for OBA and/or Multi-Site Advertising services, must adhere to the applicable

⁵⁸ 2008 Code *at* Section III.5 (b).



provisions of this Code. This requirement does not apply if that non-PII is itself proprietary data of the third party.”

Security⁵⁹

Comments Received:

One comment indicated that “security” should address “transfer” as well as collection and storage. This would include transfer of OBA and Ad Delivery and Reporting data to portable media and networks, as well as agents. In addition, one comment suggested that the NAI ought to provide greater clarity on the meaning of “reasonable security.” The NAI’s proposed security principle currently obligates members that collect or store data for use in OBA to provide “reasonable security” for that data, noting in a footnote that this standard should be determined based on several factors. The commentator encouraged the NAI to provide additional guidance by requiring that members that collect or store data for use in OBA establish, implement and maintain appropriate safeguards to protect consumers’ information, as consistent with FTC guidance on appropriate security for PII data.

Discussion:

The NAI agrees with the commentator that the same security ought to govern not only the collection and storage but the transfer of data used in OBA. The provision will be amended accordingly.

The NAI also agrees that implementation of the reasonable security standard in the NAI Code should be *informed* by existing regulatory guidance from the PII security arena. FTC guidance on PII security indeed suggests that

⁵⁹ Public Comment Draft *at* Section III.8 and n. 10; 2008 Code *at* Section III.8 and n. 9.



establishing, implementing and maintaining appropriate administrative, technical and physical safeguards involves ensuring the security, integrity and confidentiality of information; protecting against anticipated threats or hazards to the security or integrity of such information; protecting against unauthorized access to and loss, misuse, alteration, or destruction of such information; and in the event of a breach, prevent further unauthorized access, and restore reasonable integrity to the affected area. This framework is used by some of the NAI's larger members that maintain PII in databases for various services, even if that PII is not used for NAI-governed behavioral advertising products.

The security standard contemplated in the NAI's proposed principle applies to ALL data, not just PII. Indeed, the great majority of data used today by NAI members is non-PII, and the "reasonable security" framework for that type of data likely entails some adjustment to the specific detail of the FTC framework. Therefore, rather than codify today's FTC framework for PII security the NAI prefers to take this guidance as appropriate for application of the Code.

Action Taken:

Update the security provision to include "transfer" of data used in OBA: "Members that collect, transfer, or store data for use in OBA, a) Multi-Site Advertising and/or Ad Delivery & Reporting shall provide reasonable security for that data."⁶⁰

Data Retention

Comments Received:

⁶⁰ 2008 Code *at* Section III.8.



One comment suggested that the NAI adopt an additional principle around data retention. Although the NAI's proposed Notice Principle requires that members notify consumers in their privacy notices the "approximate length of time that data used for OBA will be retained by the member company," the NAI did not place any other limitations on data retention. The commentator urged the NAI to go a step further and adopt a data retention provision that limits a member's retention of any data collected for the purpose of Ad Delivery & Reporting or OBA to that time that is necessary to fulfill a legitimate business need or as required by law. That deemed "necessary" would of course differ depending on the circumstances.

Discussion:

In principle the NAI believes that the commentator's proposed standard is already at play in the marketplace and could apply equally to all data used online. It was in part for this reason that initially the NAI did not see particular value in codifying the retention framework with hard and fast rules that are currently in some flux. Also, it is unclear how a consumer would come to expect a member to apply such a principle, or how such a principle could be audited by objective means. However, the NAI acknowledges that there is some value in a retention framework for a broader range of industry participants as the NAI's membership grows. Small companies might benefit from a default retention rule that could be applied in a manner consistent with other competitors, and that would still be sufficiently flexible to allow businesses to tailor retention periods to legitimate business purposes and law enforcement requirements. This standard is aligned with the FTC's own proposed Principle on data retention.⁶¹ The NAI did not modify the standard to

⁶¹ See Staff statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Guidelines," available at <http://www.ftc.gov/os/2007/12/P859900stmt.pdf> (accessed 15 December 2008) at p. 4.



accommodate a purpose specification limitation on data retention, as suggested by some privacy commentators, because the NAI believes that consumers should be allowed to consent to secondary uses of data as circumstances change. Recall that under the NAI Code "OBA segments" may only be used for marketing purposes, whereas the raw data collected for OBA may be retained for any legitimate business or as required by law, pursuant to this provision.

Action Taken:

The NAI adopts the proposed retention standard consistent with both the FTC's December 2007 Proposed Principles and the commentator's suggestion: "Members engaged in OBA, Multi-Site Advertising and/or Ad Delivery & Reporting shall retain data collected and used for these activities only as long as necessary to fulfill a legitimate business need, or as required by law."

4. FEEDBACK ON SECTION IV

Amendments to the NAI Principles

Comment Received:

One commentator urged the NAI to formally adopt a provision reopening the Principles for active amendment every two years, as a mechanism to ensure that the Code remains a vital reflection of changing market practices.

Discussion:



As discussed earlier in this document,⁶² the NAI agrees that ongoing review of new business models and application of the Code must be undertaken. The “implementation guideline” framework, which will likely occur more frequently than every two years, should provide the flexibility of structure needed to accomplish the commentator’s suggestion.

Action Taken:

Section IV.1(b) shall be extended to incorporate the implementation guidelines process: “Membership in the NAI requires public representations that a member b) company’s business practices are compliant with each aspect of this Code that apply to its business model, as supplemented by applicable implementation guidelines that shall be adopted by the NAI from time to time.”⁶³

Public Availability

Comment Received:

One comment emphasized the importance of having policies and procedures governing annual audits to be publicly available on the NAI website, rather than be available only subject to active request.

Discussion:

The NAI agrees that the public availability of policies and procedures governing compliance reviews and annual reports of consumer

⁶² See discussion of implementation guidelines, *supra* at pp. 2-4.

⁶³ 2008 Code at Section IV.1 (b).



complaints/resolutions (in aggregate) can be made available on the NAI website, which will help reinforce the NAI's commitment to transparency of process. Accountability is tied not only to the visibility of the standards, the availability of public dispute mechanisms and referrals from consumers, regulators and advocacy groups: it is also tied to transparency of process. In the near term, concurrent with the operation of the new Code, a description of the compliance review policies and procedures adopted by the NAI will be added to the public pages of the NAI website.

Action Taken:

Section IV.1(c) shall be amended to read: "The NAI's policies and procedures for compliance reviews may be adapted from time to time, and these policies and procedures shall be made available on the NAI website." Section IV.1 (e) is amended to read: "An annual summary relating to consumer complaints received, and e) any enforcement actions taken, shall be made available on the NAI website."

Compliance Reviews

Comments received:

One commentator suggested that the NAI designee contemplated in the enforcement section to undertake compliance reviews ought to be an independent third party. Another commentator noted that the requirements, if they stay close to as written, would benefit from some illustrative examples as to what would be adequate to satisfy each of the standards, given that "the requirements as written would make even a seasoned auditor wrinkle a nose." The NAI should endeavor, to the extent possible, to establish objective, complete, relevant but also *measurable* standards.



Discussion:

Self-regulation is a model that can leverage multiple marketplace actors to constrain member companies' practices. Competitors, observers and consumers all contribute to this self-regulatory process. Effective internal and external enforcement is important not only to reassure competitors that they are being similarly constrained within a voluntary self-regulatory framework, but also to ensure the long term viability and credibility of the self-regulatory brand.

With respect to the identification of a third-party versus an in-house "designee" for compliance reviews, under the Code the NAI retains the flexibility to identify a designee of its choice to undertake execution of the policies and procedures articulated for this purpose. However, the NAI has surveyed major privacy self-regulatory programs and has found that self-regulatory organizations most commonly enforce policies themselves against their members' and/or seal holders' attestations. No example to the contrary was offered up by commentators.

Furthermore, significant PII self-regulation in other legal contexts also relies heavily on the self-attestation framework. Like these other programs, the NAI places principal reliance on the binding nature of extensive self-attestations made by virtue of publication of NAI membership itself. Such representations are subject to enforcement under Section V of the FTC Act by the Federal Trade Commission, and such enforcement is contemplated within the NAI self-regulatory structure. Compliance review of company attestations by the NAI itself, rather than government action, is intended by the NAI as the primary means of enforcement. By establishing policies and procedures for compliance reviews and complaint management, and by assigning duties to NAI designees to carry out these requirements, the NAI mirrors the common



privacy self-regulatory model employed by several other organizations.⁶⁴ Another notable example of this approach is the EU Safe Harbor program, which applies to EU personal data transfers to the US. By mirroring an attestation model that is widely recognized as suitable for personal data transfers (even though much of the data used by members for behavioral advertising is non-PII) the NAI believes it can achieve an accountability regime that is appropriate for the nature and scope of the matters it regulates. By further layering on a pre-certification review and annual verification process undertaken by NAI staff against those member attestations, which have lengthened since the NAI's 2000 program began, the NAI can further reinforce the validity of the self-attestation model.

Certain attributes of the NAI program are legacy items from deliberations in 2000 that remain relevant in the marketplace today. That said, it is true that many of the provisions that are not related to public disclosures or choice mechanisms are business practice limitations that nevertheless require a member to "certify" or "attest" to the fact that it is *not* engaging in a certain activity. Such provisions are indeed less of a concern for the annual compliance review than those that are more objective, verifiable and measurable. However, such attestations provide a more diverse basis for public accountability and as such play a useful role in a self-regulatory framework that seeks to leverage Section V FTC Act liability. The NAI agrees that to the extent feasible, the NAI must endeavor to provide its compliance review designee and members alike with examples of model implementations for each provision, representing at least one example that should be deemed compliant with the given standard.

⁶⁴ See, e.g., Direct Marketing Association's Guidelines for Ethical Business Practice program, at <http://www.dmaresponsibility.org/Guidelines/> (accessed 15 December 2008); TRUSTe's Watchdog Dispute Resolution and Appeals Process, at <http://www.truste.org/consumers/compliance.php> (accessed 15 December 2008); Entertainment Software Ratings Board Privacy Online Program at http://www.esrb.org/privacy/privacy_enforcement.jsp (accessed 15 December 2008).



Action Taken:

The NAI will provide its compliance review designee and members alike with examples of model implementations for each provision, representing at least one example that should be deemed compliant with the given standard. These examples are not themselves intended to be construed as requirements.

CONCLUSION

The significant task of updating a Self-Regulatory Code of Conduct cannot be accomplished without countless hours of work and a spirit of collaboration and compromise. The members of the Network Advertising Initiative, joined by ever increasing numbers of peers since this process was first announced in January 2008, have remained diligently committed to reaching consensus and addressing concerns raised about behavioral advertising in a candid and transparent manner. As always, NAI staff are available to answer questions about the 2008 Code from interested parties or prospective members. Contact information is available on the NAI website, at <http://www.networkadvertising.org>.

NAI Full Compliance Members (as of 12 December 2008)

Acerno (www.acerno.com) is the predictive targeting network that drives consideration for brands, incremental transactions for retailers, and relevance in advertising for consumers. No personal information of any kind is ever collected: We use analytics and completely anonymous shopping data to accurately describe audiences and predict what they are interested in buying.

Advertising.com (www.advertising.com) operates the largest display advertising network in the United States and is part of Platform-A, AOL's advertising business.

Akamai Technologies, Inc. (www.akamai.com) provides market-leading managed services for powering rich media, dynamic transactions, and enterprise applications online. Some of these services help publishers and advertisers from across Akamai's



customer base to better understand their consumer end users and to provide more personalized on-line experiences, including by better targeting advertising. To learn more about Akamai's commitment to privacy, [please click here](#).

AlmondNet (www.almondnet.com) Founded in 1998, AlmondNet is a New York-based media and advertising technology company that revolutionizes search and makes the Internet advertising market efficient by distributing relevant paid search ads to people wherever they go, based on recent searches they made.

Atlas (www.AtlasSolutions.com) is an online advertising product operated by Microsoft Corporation. Via Atlas, Microsoft provides digital marketing technologies that are designed by marketers, for marketers. This buy-side focus enables Atlas to develop effective tools and services that meet the real-world needs of agencies and advertisers. Microsoft, along with its family of companies, considers Internet user privacy to be of paramount importance. We are committed to protecting users' online privacy and have implemented a progressive privacy policy.

BlueKai (www.bluekai.com) is the creator of the first and largest online data exchange that is designed with consumer transparency and participation in mind. Unlike ad networks, BlueKai does not sell ads or impressions. By aggregating valuable shopping and research data across the Internet, BlueKai enables marketers and ad networks to drive effective and scalable targeting and prospecting campaigns. Publishers can participate as intent data providers to earn revenue in a privacy friendly way. Our goal is to create the next-generation approach to effective online marketing that is driven by intent data and advocacy for consumer participation.

BlueLithium (www.bluelithium.com) is a Yahoo company. Yahoo! Inc. is a leading global Internet brand and one of the most trafficked Internet destinations worldwide. Yahoo! is focused on powering its communities of users, advertisers, publishers, and developers by creating indispensable experiences built on trust. Please visit www.bluelithium.com to learn more about BlueLithium's commitment to privacy.

Dedicated Networks (www.dedicatednetworks.com) is an online advertising platform allowing advertisers to effectively reach their target audience, while maintaining brand response and direct response goals. Dedicated Networks incorporates custom channel targeting within its list of 2,000+ publishers, reaching more than 90MM unique users.

FetchBack (www.fetchback.com) is the Retargeting Company that converts more lost prospects than any other Retargeting solution in the marketplace today. We are dedicated to protecting consumer privacy online.

The Fox Audience Network (www.foxaudienzenetwork.com) enables marketers of all sizes to find and connect with customized audiences across the Internet. With its massive



reach and the industry's leading customization and reporting platform, FAN is able to maximize return on investment for marketers and revenues for publishers while creating an altogether more relevant experience for users across the web.

Google (www.google.com) operates the DoubleClick online ad serving product, providing advertisers, web publishers and direct marketers with the tools needed to plan, execute and analyze marketing programs with greater ease and efficiency. Our comprehensive set of integrated solutions have become leading tools for campaign management, online advertising, email delivery, offline database marketing, data management and marketing analytics. As consumers embrace new forms of media and business scales to meet the demands of multi-channel marketing, Google will remain at the forefront, helping marketers effectively target, reach and measure the results of their marketing programs.

interCLICK (www.interclick.com) is the leading transparent ad network, committed to providing full end-to-end transparency to advertisers, publisher and consumers. In 2007, comScore named interCLICK the fast growing ad network and currently reaches over 65% of the U.S. internet audience and growing. interCLICK provides advertisers solutions for the entire marketing lifecycle, employing the latest advanced targeting methodologies to meet and exceed campaign goals. With a network of comScore top 1000 sites, top brand advertisers and consumer choice, interCLICK strives to be a trusted partner for all of its clients. For more information, please visit www.interCLICK.com.

Media6° (www.media6degrees.com) provides marketing analytics to help leading marketers meet their online customer acquisition goals. Our proprietary targeting technology delivers behaviorally targeted banner ads across the web. For more information about our privacy practice, please visit our privacy policy <http://www.media6degrees.com/privacy.php>.

Mindset Media (www.mindset-media.com) is the internet ad network for brands. Using its proprietary psychographic standard, Mindset Media lets brand advertisers target millions of people with the personality traits that fit their brands in simple online media buys.

Revenue Science, Inc. (www.revenuescience.com) provides relevant advertisements to consumers based on your interests. In order to provide advertisements that may be of interest to you, Revenue Science uses general information about the types of Web sites you visit and other non-personally identifiable information about you. Revenue Science, along with its affiliated publishers and advertisers, holds the privacy of its users in the strictest confidence. At no time is personally identifiable information associated with any behavioral data in the Revenue Science Audience Search Network. All information gathered by Revenue Science remains the sole property of our customers. Please see our privacy policy for additional information on our product and privacy practices.



Safecount (www.safecount.net) provides a simple, straightforward digital platform that enables advertisers, researchers and media companies to understand the effectiveness of online advertising and marketing programs. The platform also gives consumers far more information about their role in these programs more plainly than ever before through a unique "cookie viewer," the first of its kind. Safecount's guiding principle is that consumers have a right to control and choose what information they share while online. We believe in being clear and transparent regarding our privacy practices, and we consider all Web visitors' opinions to be very important. Safecount is committed to promoting respect for consumer privacy and consumer control in collaboration with online researchers, advertisers and publishers. For more information, please visit: www.safecount.net.

SpecificMEDIA, Inc. (www.specificmedia.com), the advertising industry's fastest-growing interactive media company, enables advertisers to target consumers through advanced demographic, behavioral, contextual, geographic and retargeting technologies. The company's Premium Network is wholly comprised of over 450 name brand publisher that reach more than 118 million U.S. consumers monthly. In addition, Specific Media's Data Network provides anonymous consumer tracking information from more than 2 million websites and 20 million web pages. The combined size of its Premium Network and Data Network enables the company to identify and target a larger number of consumers than other networks. Specific Media works with leading Fortune 500 brand advertisers, including seven of the top 10 companies. No other media company gives advertisers the ability to reach their target audience online with scale and nearly 100% accuracy.

Tacoda (www.tacoda.com) is the world's most advanced behavioral targeting advertising network and powers the behavioral targeting solution offered by Platform-A, AOL's advertising business.

Traffic Marketplace (www.trafficmarketplace.com) As the premiere Business-to-Audience online ad network, Traffic Marketplace delivers relevance in online advertising by connecting advertisers with their target audience.

Traffic Marketplace delivers billions of advertising impressions each month to over 120 million unique US users, generating millions of leads and customers from its network of top tier branded websites.

Tribal Fusion (www.tribalfusion.com), a leading site representation company, partners with top quality web publishers to provide both brand and direct advertisers with targeted ad placements. Offering site-specific, channel-wide, run-of-network ads as well as behavioral and contextual placements, Tribal Fusion delivers results through expert advice and intelligent technology.



Tribal Fusion is part of the Exponential Interactive Inc. group of online marketing businesses. Tribal Fusion, along with its sister companies, is committed to protecting users' online privacy. For additional information, please see our [privacy policy](#).

Turn Inc. (www.turn.com) is an innovative technology company that provides advertisers and publishers with an advanced marketplace for buying and selling online advertising. Turn's technology utilizes information about the publisher, web page, advertiser and anonymous audience to improve the relevance of the advertising shown to you. Turn cares about consumer privacy and our technology does not collect or utilize your name, address, email or any other personally identifiable information. For information about Turn's privacy practices, please visit our [privacy policy](#).

24/7 Real Media Inc. (www.247realmedia.com) is a leading global digital marketing company, empowering advertisers and publishers to engage their target audiences with greater precision, transparency, and ROI. Using its award winning ad serving, targeting, tracking, and analytics platform, powerful search marketing capabilities and global network of specialized Web sites, the company has turned the art of reaching audiences across virtually any digital medium into a measurable science.

Undertone Networks (www.undertone.com) is a premier online advertising network comprised of today's top media properties. Undertone executes and manages online advertising campaigns for leading digital and traditional advertising agencies along with the marketers they serve. We provide online solutions that help advertisers achieve their brand and performance-based initiatives via a comprehensive selection of ad formats, rich media, and targeting capabilities, combined with expert, personalized service and an unwavering dedication to reliability and accountability.

[x+1] (*formerly Poindexter Systems, Inc.*) (www.poindextersystems.com) is the new standard in behavioral targeting. The company's performance optimization technologies enable marketers to maximize the performance and profitability of their online marketing efforts. The company's Progressive Optimization Engine™ (POE) is the industry's first real-time statistical modeling platform that uses clustering and predictive modeling to identify audience viewing behavior and automatically deliver the right message to maximize response through any digital channel.

Yahoo! Inc. (www.yahoo.com) is a leading global Internet brand and one of the most trafficked Internet destinations worldwide. Yahoo! is focused on powering its communities of users, advertisers, publishers, and developers by creating indispensable experiences built on trust. Please visit the Yahoo! Privacy Center to learn more about Yahoo!'s commitment to privacy across its diverse products and services.