

## FTC Proposes Online Behavioral Advertising Privacy Principles: Extend Far Beyond NAI Principles Approved in 2000 – Comments Due February 22, 2008

### INTRODUCTION

On December 20, 2007, the Federal Trade Commission (“FTC”) staff released for public comment proposed online behavioral advertising privacy principles (“Principles”) in an effort to guide self-regulation of this nascent industry.<sup>1</sup> The proposed Principles, described in detail below, are stringent and extend far beyond the Network Advertising Initiative’s Principles For Online Preference Marketing approved by the FTC in 2000. Moreover, they would apply to a very wide array of online activity. Specifically, the FTC staff proposes a broad definition of “behavioral advertising” that includes “the tracking of a consumer’s activities online including the searches the consumer has conducted, the web pages visited, and the content viewed in order to deliver advertising targeted to the individual consumer’s interests.”<sup>2</sup> Notably, this definition includes not only cross-site tracking, such as that used by network advertisers, but also single-site or domain tracking that is now commonly used by website operators to personalize their sites’ content and advertising.

Comments on these proposed Principles are due by February 22, 2008. The final Principles that emerge from this process will be important for two reasons: (1) they will have a strong influence in shaping the modification of existing self-regulatory regimes or in the development of new self-regulatory regimes; and (2) while couched as proposals for self-legislation, they give a picture of the FTC staff’s view of appropriate practices for behavioral targeting, and perhaps even the staff’s view on standards necessary to comply with § 5 of the FTC Act. It is very important for the industry to comment in detail on the proposal because, as written, its combination of high standards in some areas and vague guidance in others has the potential to threaten the viability of most forms of behavioral targeting used today.

While the FTC recognizes that behavioral advertising provides a number of benefits to consumers, it is important to understand that these proposed Principles are based on the FTC staff’s premises that: (1) consumers are unaware of behavioral advertising practices or cannot discern when such practices are

---

<sup>1</sup> See FTC, Press Release, *FTC Staff Proposes Online Behavioral Advertising Privacy Principles*, at <http://www.ftc.gov/opa/2007/12/principles.shtm>.

<sup>2</sup> FTC, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, at 2, at <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

used; (2) transparency and consumer autonomy are critical to consumer trust and the online marketplace; and (3) data collected for behavioral advertising may fall into the wrong hands or be used for unanticipated purposes.

With these assumptions as a backdrop, the Principles include:

• **Transparency and Consumer Control:**

- **Notice:** “A clear, concise, consumer-friendly, and prominent statement”<sup>3</sup> disclosing that consumer data is collected for behavioral advertising and that consumers can decide whether such collection is permitted. Under the proposal, this disclosure would be located on every website where consumer data are collected for purposes of behavioral targeting; and
- **Consumer Choice:** “A clear, easy-to-use, and accessible method”<sup>4</sup> to stop these data collection practices, also displayed clearly and prominently on the web publisher’s site.

These Principles alone appear to be more stringent than the current Network Advertising Initiative principles for notice of behavioral targeting using anonymous data, which allows for notice and an opt-out to be in the web publisher’s privacy policy. Under the Principles proposed by the FTC staff, notice and choice would appear to be required on the website itself, in a prominent way, like any other disclosure, unless restricted by industry comment. Commenters should focus on whether this standard is realistic and whether it would unnecessarily

retard the growth and development of behavioral targeting.

• **Data Security:** Under the proposed Principles, companies that collect and store data for behavioral advertising purposes would be required to provide security consistent with data security laws and FTC data security enforcement actions and guidance. Thus, the proposed Principles call for data security that is appropriate considering the type of data collected, the nature of the company’s business, the risks faced, and the reasonable protections available. This standard would apply even for anonymous data used for behavioral targeting. Comments on whether such a standard is appropriate for anonymous data that cannot be linked to PII would help the FTC staff in creating a Final Proposal.

• **Data Retention:** The proposed Principles call for companies to retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. This principle, borrowed from FTC law enforcement cases in information security, is not part of the existing NAI self-regulatory regime. It appears that the Commission staff would like to see a sliding scale for data retention timeframes depending on the type and sensitivity of the data and the usefulness of the data for purposes of behavioral advertising over time. Companies are welcome to – and should – comment on whether such a standard is reasonable for anonymous data that cannot be linked to PII and what specific minimum retention periods are appropriate in order to avoid business risks associated with being required to destroy data too soon.

---

<sup>3</sup> *Id.* at 3.

<sup>4</sup> *Id.*

• **Changes to Privacy Policies:** The proposed Principles borrow from previous FTC privacy cases by suggesting that companies should obtain affirmative express consent from consumers before using consumer data in a way that is materially different from the uses permitted under the privacy policy in place when the data were collected. This has important implications for behavioral advertising to the extent a behavioral advertising company proposes to run its ads on websites that have policies that are silent on behavioral advertising. Would opt-in be required in that instance? Right now it is unclear, and comments on how this very stringent requirement – affirmative express consent – would work in practice under a variety of scenarios and preexisting privacy representations by web publishers, and whether it would unnecessarily stunt the growth and development of this new and very promising industry, will help shape the final FTC staff Proposal.

In any event, opt-in is an extremely high standard, and commenters should ask for more clarity on what should be a relatively rare requirement, and one which would be extraordinary for any business. Comments should urge that for opt-in, the definition of “material” should be specific, and should focus on things like direct contradictions to previous representations in privacy policies as opposed to simply addressing a use that is unaddressed in the existing policy.

• **Sensitive Data:** The FTC staff further proposes, in broad strokes, that a company should obtain affirmative express consent

before collecting sensitive data for behavioral advertising. The FTC staff acknowledges the difficulty inherent in defining “sensitive information” in this context, and therefore asks for comment on: (1) what types of information should be considered “sensitive” (and therefore subject to a higher standard for use in behavioral targeting); and (2) whether targeting using this information should be prohibited outright instead of limited to consumer choice. Comments on the types of categories that should be allowed for behavioral targeting will be very helpful to the staff, and may serve to save some relatively benign categories from unnecessarily strict regulation.

**Call for Additional Information:  
Using Tracking Data for Purposes  
Other than Behavioral Advertising**

The FTC staff is also interested in secondary uses of consumer data and seeks commentary on which secondary uses raise concerns, whether these uses are practiced, whether the concerns apply to non-personally identifiable information, and whether heightened protection is merited.

**FOR MORE INFORMATION**

For more information about this Client Advisory, please contact:

**D. Reed Freeman, Jr.**  
**(202) 342-8880**  
**[rffreeman@kelleydrye.com](mailto:rffreeman@kelleydrye.com)**