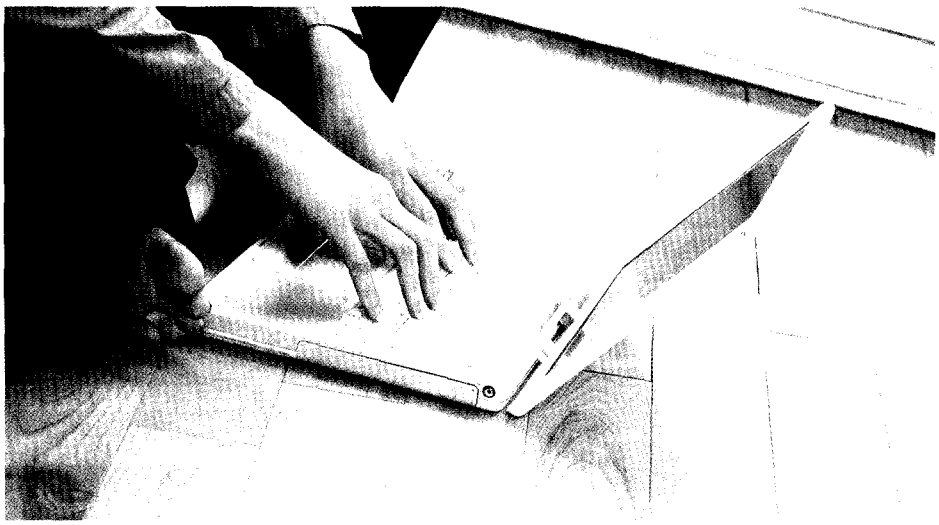
Online Behavioral Tracking: Implications of Regulation

By Howard Fienberg



Driven by consumer fears of online targeted advertising, Congress, the Federal Trade Commission (FTC) and several state governments continue to consider regulating and restricting the collection and sharing of even non-personally identifiable information on the Internet, such as IP addresses and cookies. This data is essential to the conduct of much research online, as well as emerging methods of respondent validation and verification essential to data quality efforts for online panels. While legislators and regulators don't intend to curtail online research, vague wording and misunderstanding of ever-more complex and advancing technologies and methods are putting online research at risk.

Behavioral targeting (also known as preference marketing, behavioral advertising, behavioral marketing or online profiling) is defined by the FTC as "the tracking of a consumer's online activities over time– 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."

MRA still wants the FTC to flesh out and clarify this admittedly "broad definition" of behavioral advertising, because as currently conceived it could include and restrict behavioral tracking for legitimate research purposes (especially if such research could be used for evaluating or constructing advertising). We continue to seek an explicit exemption for behavioral tracking for research purposes.

What Some Activists Want: A Do Not Track Registry

Numerous privacy activist groups have been advocating that the FTC set up a Do Not Track Registry to let consumers explore the Internet shielded from behavioral tracking. Registry advocates have compared it to the national Do Not Call Registry, but compiling and applying the list would be exceptionally difficult and registry compliance would be prohibitively expensive.

The proposed Do Not Track Registry would make no useful distinction between tracking data collected for research, transactional, political, governmental or commercial/sales purposes. Such distinctions are the cornerstone of the extremely popular Do Not Call Registry, which shields consumers who so request shielding from unrequested telemarketing telephone calls, while allowing calls for survey/opinion purposes.

What Has Happened So Far

The FTC held an "Ehavioral Advertising Town Hall" on the subject in November 2007 (at which a member of the MRA Government Affairs Committee, George Pappachen of the Kantar Group, presented on a panel), followed by the issuance a month later of the FTC's proposed "Self-Regulatory Principles." We submitted comments, to which the FTC paid some attention before filing their final version of the Principles in February 2009.

What You Need to Know About the FTC's Principles

The first is transparency and control: companies that collect information for behavioral advertising should provide meaningful disclosures to consumers about the practice and choice about whether to allow the practice. The second principle proposes reasonable security and limited data retention: companies should provide reasonable data security measures so that behavioral data does not fall into the wrong hands, and should retain data only as long as necessary for legitimate business or law enforcement needs. The third principle governs material changes to privacy policies: before a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the consumer. The fourth principle states that companies should obtain affirmative express consent before they use sensitive data – for example, data about children, health or finances – for behavioral advertising.

The first three principles are broadly consistent with existing law (and FTC interpretation and enforcement), although MRA remains severely concerned with the fourth, particularly because (1) the

FTC has yet to properly clarify what makes information sensitive and (2) existing U.S. law does not require affirmative express consent for most such data.

In refining what the agency considers to be behavioral advertising, the final report essentially exempts "first party" or "intra-site" behavioral tracking because it constitutes an understandable and "direct relationship" between the Web site and the user. The FTC also believes that "first party" data collection may be necessary for many "consumer benefits and services," as well as "security measures, fraud prevention and legal compliance." The FTC also exempts "contextual" advertising in the final report, which is delivered "based only on the content of a particular Web site or search query, rather than on information about the consumer collected over time."

Unlike the original proposal, the FTC now limits the scope of information collection of concern to only data that "reasonably could be associated with a particular computer or device." However, this definition of Personally Identifiable Information (PII) is much broader than it sounds and would include: "clickstream data that, through reasonable efforts, could be combined with the consumer's Web site registration information; individual pieces of anonymous data combined into a profile sufficiently detailed that it could become identified with a particular person; and behavioral profiles that, while not associated with a particular consumer, are stored and used to deliver personalized advertising and content to a particular device."

Also, the FTC says that every Web site that collects data for behavioral tracking should provide site users with "a clear, concise, consumer-friendly and prominent" disclosure of such data collection, and a "clear, easy-to-use and accessible means" for users to choose whether or not to have their data collected for delivering targeted advertising. While this is not an opt-in standard, the FTC recommends that this disclosure and choice be relayed through more creative ways than the standard privacy policy, which the FTC laments may no longer be an effective way to share information with Web users given policies' length and complexity.

The FTC further criticizes reliance on the use of cookies for opt-out methods, since privacy settings and other tools frequently delete or block cookies that can remind a Web site or service that a user has opted out of data collection. What the next technological leap will be that replaces cookies remains unclear. Based on the continued aversion to cookies by privacy activist groups and the FTC, it is not unlikely that this next technological leap will be similarly targeted shortly after it comes into use.

Self-Regulatory Efforts Underway

While MRA has specifically covered behavioral tracking in our Code of Ethics, we are keeping an eye on self-regulatory efforts across other industries, such as the Network Advertising Initiative (NAI) standards for behavioral tracking late last year, an assessment tool release by the Center for Democracy and Technology (CDT), new tools from Google and Yahoo! to allow users to opt out of targeted advertising and the newest version of Microsoft's Internet Explorer, which will include tools to prevent the accumulation of behavioral data online.

(Continued on page 40)

(Continued from page 39)

Not Just an Issue in the U.S.

The European Union Consumers Commissioner Meglena Kuneva, at a recent roundtable discussion on online data protection, criticized online behavioral targeting as "increasingly pervasive," noting that "consumers understandably feel uncomfortable." Like the FTC, she has called for self-regulatory "principles of acceptable behavior."

What Next?

While the FTC's Principles are only "guidelines" for how industry should regulate itself, new FTC Chairman Jon Leibowitz said, "This could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy."

Not interested in waiting to see, legislators in Connecticut (A. 1393), Massachusetts (H.B. 4822) and New York (S. 616) have introduced legislation to restrict behavioral tracking.

In Congress, Rep. Rick Boucher (D-VA), Chairman of the Energy and Commerce Committee's Telecommunications and the Internet Subcommittee, is considering legislation to more broadly eliminate the "self" from "self-regulatory" on this issue. Upon the final Principles' release, Rep. Boucher remarked, "At a minimum, it is important that consumers understand what information is collected by Web sites, to show how that information is used, and then to be able to let consumers make choices about whether or not that information is collected and whether or not it is used in a certain way." Senator Byron Dorgan (D-ND) has also expressed interest.

MRA will be working with Rep. Boucher, Senator Dorgan, other Congressmen, and state legislators to ensure that any legislation protects the interests of the research profession.

Resources:

- CMOR-filed Comments on FTC's Proposed Principles: http://www.ftc.gov/os/comments/behavioraladprinciples/080411cmor.pdf
- FTC Self-Regulatory Principles For Online Behavioral Advertising: http://www.ftc.gov/opa/2009/02/behavad.shtm
- Network Advertising Initiative (NAI) Self-Regulatory Standards: http://www.networkadvertising.org/networks/principles_comments.asp
- CDT Threshold Analysis for Online Advertising Practices: http://www.cdt.org/privacy/20090128threshold.pdf
- EU Consumers Commissioner's Remarks: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/156&format=HTML&aged=0&language=EN&guiLanguage=en

Disclaimer: The information provided in this article is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. MRA advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

Howard Fienberg is the director of government affairs at MRA.