INTELLECTUAL PROPERTY ALERT

ROBINSON BRADSHAW & HINSON

APRIL 2009

Behavioral Advertising: The Next Frontier for Privacy Law?

By John M. Conley

The practice of "behavioral advertising"—tracking consumers' online activities in order to deliver advertising tailored to their interests—has been unregulated until now. But it appears that regulation may be imminent, both in the United States and internationally. Plaintiffs' class action lawyers are also showing interest. It may be time for everyone involved, from Internet service providers to individual advertisers, to assess their practices in order to get out ahead of the law. The measures that should be taken are relatively simple, and in any event far simpler than defending a class action.

Congress held hearings on behavioral advertising last year, and members' questions reflected particular concern about "deep-packet inspection"—a technology that tracks every Web site that particular consumers visit and generates extremely detailed information about their purchases, travel habits, how much they spend, and even what credit cards they use. The same issues have dominated additional hearings this spring, and many observers expect federal legislation this year. Behavioral advertising has already provoked two class action lawsuits, both filed in California. The suits claim that Internet advertising companies—NebuAd in one case, Adzilla in the other—purchased deep-packet information from consumers' ISPs and planned to use it to serve them targeted ads. The plaintiffs in both cases are asking the court to approve classes that include all affected consumers. A number of national and regional ISPs are named as defendants, and the plaintiffs have used an unusual California procedure called "John Doe defendants" to leave open the possibility of adding even more.

The two suits allege that deep-packet inspection violates a long list of state and federal privacy, consumer security, and wiretap laws. The plaintiffs' lawyers stress that the inspection took place without the consumers' knowledge or consent, while the defense lawyers contend that the plaintiffs have not been damaged. They claim that the defendants did not know who the individual consumers were, and planned to do nothing more than show them products and services in which they might be interested. It is far too early to say whether the plaintiffs will prevail, or even whether the courts will allow the cases to proceed as class actions. But there has been a practical impact: Adzilla has stopped doing business in the U.S., while NebuAd gave up on its plan. In any event, even a meritless class action imposes major expense and burden on the defendants.

The Federal Trade Commission has now entered the fray. The FTC has previously asserted authority to regulate data security and other aspects of privacy under section 5 of the FTC Act, a broad prohibition of unfair or deceptive trade practices. In February, the Commission issued revised "Self-Regulatory Principles for Online Behavioral Advertising." Although the principles are voluntary at this point, one of the commissioners warned that "this could be the last clear chance to show that self-regulation can—and will—effectively protect consumers' privacy." Privacy advocates have already condemned the voluntary guidelines as too weak, and many expect the FTC to take a mandatory approach in the near future.

There are four principles. First, Web sites should provide clear and conspicuous notice of behavioral advertising, and a simple way for consumers to choose whether to participate. In announcing this principle, the FTC criticized typical posted privacy policies as "long and difficult to understand," and urged companies to do better. Second, companies should provide reasonable security for data they collect for behavioral advertising and retain it only as long as necessary to fulfill legitimate business needs. Third, changes in behavioral advertising policies should be given prominent notice that includes a consumer opt-out choice. The fourth principle reflects heightened concern with sensitive information, including that pertaining to health, finances, or children, and urges companies to obtain express consent before collecting it.

The FTC's approach is part of an international trend. In a recent speech, the European Union's consumer affairs commissioner criticized many companies' behavioral advertising policies as hard to understand, with consumer opt-out provisions too difficult to find. She singled out Facebook for its practice of sharing data with commercial partners that are not bound by its policies, and hinted that more aggressive law enforcement is coming. In apparent anticipation of such a development, a consortium of British Internet advertisers has adopted "best practices" guidelines that look very much like the FTC's principles.

In this rapidly evolving legal environment, the most sensible approach is for everyone involved in Internet advertising to assume that something at least as strong as the FTC's principles is likely to become law in the relatively near term, either by Congressional legislation or direct FTC action. Compliance with the principles is as close to a legal safe harbor as there is right now. ISPs, those in the business of creating or selling behavioral advertising, and companies that otherwise cooperate in the collection of behavioral data, are obvious candidates for immediate compliance. But even companies that merely buy behaviorally targeted ads for their products should ask hard questions of those who are selling that service. Far better to be cautious now than to have to extricate oneself from an FTC suit or class action later.