JANUARY 2011

FEDERAL GOVERNMENT CALLS FOR MORE INTENSIVE REGULATION OF ONLINE BEHAVIORAL ADVERTISING

Recently, the Federal Trade Commission (among others) has suggested a need for more intensive regulation of online behavioral advertising. The chief object of such regulation is to ensure that consumer privacy is protected and that abuses of consumer information do not occur. Others have suggested that self-regulation, or a system of public and private litigation aimed at curbing excesses in information-gathering practices, may better address these central concerns while maintaining the economic viability of behavioral advertising.

The modern, commercial internet grew up with advertising as a core feature. "Banner" advertisements first appeared in the early 1990s. By the late 1990s, "pop-up" advertisements became prevalent. Today, more than 1 billion people use the internet, and U.S. online sales alone approach $1 trillion per year.

By the late 1990s, "online profiling" (later called "behavioral advertising") began its rapid development. This practice held the promise of "reinventing" the marketing process, producing "targeted" advertising that takes into account prior online behavior in order to present consumers with goods and services they were most likely to buy. Today, the gathering of online behavioral data has become nearly ubiquitous. As technologies converge, and internet services are increasingly provided over cellular telephones and other mobile devices, the ability to locate consumers physically (through GPS functions) may soon generate location-based advertising, keyed to where a person is at any given moment. Targeted advertising also has begun to appear in online games, social media, and blogs.

The FTC held its first public workshop on online privacy in 1995 and issued a major report to Congress in 2000.[1] In its 2000 report, the FTC recognized the potential benefits that online profiling might offer to internet users, but it also noted "widespread" concerns about collection of personal data, including

1 *See* FTC, *Online Profiling: A Report to Congress* (June 2000), www.ftc.gov.

the risk that behavioral profiling may be "conducted without consumers' knowledge." The report recognized the FTC's "longstanding support" of industry self-regulation but suggested a need for "backstop" legislation to "set forth a basic level of privacy protection." Congress, however, chose not to enact such a law.

In 2007, the FTC proposed a set of (voluntary) principles for online information-gathering.[2] In 2008, the Network Advertising Initiative ("NAI"), first formed in 2000, issued its own self-regulatory principles for privacy practices.[3] An additional set of self-regulatory principles appeared in 2009.[4]

Late in 2009, the FTC commenced a three-part roundtable series, "Exploring Privacy," meant to review virtually every aspect of consumer privacy in the modern technology and business environment. FTC Chairman Jon Leibowitz, in introducing the series, called the inquiry a "watershed moment in privacy" and suggested that, because "consumers don't read privacy policies," and because "unbelievable advances in technology" permit companies to "store and crunch massive amounts of data relatively cheaply," the current regulatory system requires review.

In December 2010, the FTC staff issued a preliminary report, aimed at providing a "broad privacy framework to guide policymakers, including Congress and industry."[5] The Report included nearly 80 pages of analysis, plus more than 60 questions on which the FTC sought additional input. The Report did not limit its focus to behavioral advertising online. Rather, the Report called for a wholesale "re-examination" of the nation's approach to privacy protection.

The FTC noted that the "limitations" of the "notice-and-choice" model have become increasingly apparent. Privacy issues have become "larger, more complex," and often "incomprehensible to consumers." While many companies offer disclosure of their practices, fewer "actually offer consumers the ability to control these practices." As a result, the FTC suggested, "consumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered [.]"

Further, the FTC noted that its "harm-based" approach to privacy protection "also has limitations." Such an approach "focuses on a narrow set" of privacy-related harms, those that "cause physical or economic injury or unwarranted intrusion into consumers' daily lives," but "the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'" Thus, the FTC suggested "[w]hen data is collected for one purpose and then treated differently, the failure to respect the original expectation constitutes a cognizable harm."

The FTC emphasized the "nearly ubiquitous" collection of consumer data and that data collectors "share the data with multiple entities" due to "economic incentives [that] drive the collection and use of more and more information about consumers." The FTC also expressed concern with the increasing erosion of anonymity on the internet.

The FTC advanced three "major elements" in its "proposed new framework for consumer privacy." First, companies should promote privacy "at all stages" of the design and development of their products and services. Second, the FTC called on companies to "simplify consumer choice." One important element of this simplification involves identification of a limited set of "commonly accepted practices" (generally related to the fulfillment of a customer order) for which companies "should not be required to seek consent once the consumer elects to use" a product or service. For practices that require consumer choice, the FTC suggested that companies should offer the choice "at a time and in a context" in which consumers make decisions about their data. Apropos existing consent-gathering mechanisms, the FTC suggested that industry efforts had "fallen short" and recommended a "Do Not Track" program, modeled on, but technically different from, the FTC's existing "Do Not Call" protective system for unwanted telemarketing.

---

2 FTC, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 2007), www.ftc.gov.
3 NAI, *Self-Regulatory Code of Conduct*, 2008, www.networkadvertising.org.
4 *See Self-Regulatory Principles for Online Behavioral Advertising*, 2009, www.iab.org.
5 *See* Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010), www.ftc.gov.

Finally, regarding means to increase the "transparency" of data practices, the FTC called for efforts to "simplify" consumer choices. The FTC also suggested that companies should provide "reasonable access" to the consumer data they maintain, with access to be "proportionate to the sensitivity of the data and the nature of its use." The FTC called for "affirmative express consent" before companies use consumer data "in a materially different manner than claimed when the data was collected." The FTC suggested that "all stakeholders" should provide "greater consumer education to increase consumer awareness and understanding" of data collection practices and their privacy implications.

Shortly after the FTC released its 2010 report, the Department of Commerce issued its own report.[6] The Commerce report, like the FTC report, suggested that a "new approach" to privacy protection may be necessary. The report cited a need for "[f]oundational principles" to "strengthen commercial data privacy," and recommended "broad adoption" of "Fair Information Practice Principles" to "help close gaps in current policy, provide greater transparency, and increase certainty for business." The report recommended creation of a "privacy office" within the Department of Commerce, to work with other agencies (including the FTC) to "convene multi-stakeholder discussions," and to "lead an international outreach" for development of commercial data privacy policies.

The Commerce Report also noted an "Administration-wide effort" to "articulate principles of transparency, promot[e] cooperation, empower[ ] individuals to make informed and intelligent choices, strengthen[ ] multi-stakeholder governance models, and build[ ] trust in online environments." Among other things, the report noted the formation (in October 2010) of a National Science and Technology Council Subcommittee on Privacy and Internet Policy, co-chaired by Cameron Kerry, General Counsel at the Department of Commerce, and Christopher Schroeder, Assistant Attorney General for Legal Policy.

Over the course of 2010, moreover, congressional committees held three hearings on issues related to online privacy (including the FTC's "Do Not Track" proposal), and at least one bill (titled the "BEST PRACTICES Act") was introduced (but not passed).[7] Legislative sponsors suggest that further online privacy bills almost certainly will be introduced in 2011.

The legislative solution proposed (to date) generally would require that companies collecting personal information about an individual clearly disclose their privacy policies and establish procedures to ensure the accuracy and security of information. Although companies may be permitted to obtain consent for the gathering of information through an "opt out" system, some form of affirmative "opt in" consent would be required for distribution of information to third parties, for the gathering of sensitive information about an individual, and for material retroactive changes in a company's privacy policies. Affirmative consent would also be required for collection of "all or substantially all" of a person's online activity.

Finally, the proposed legislation calls for enforcement of the law by the FTC, granting the FTC rulemaking authority and granting concurrent enforcement authority to state attorneys general, with a private right of action if a company "willfully fails" to comply. The legislation would also establish a form of "safe harbor" for companies that engage in an FTC-approved self-regulatory program.

The coming year will almost certainly see additional reports by the FTC and the Commerce Department, as well as introduction of further legislative proposals in Congress. Equivalent state developments may also advance. Indeed, in the "lame duck" session of Congress at the end of 2010, Congress passed (and the President signed into law) the "Restore Online Shoppers' Confidence Act," which aims at protecting consumer financial information online.

Companies interested in this subject should consider commenting on the FTC and Commerce Reports.[8] We expect to produce additional commentary on any further agency reports or legislative initiatives.

---

6 *See* Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy in the Internet Economy: A Dynamic Policy Framework* (Dec. 2010), www.ntia.doc.gov.

7 *See* H.R. 5777 (sponsored by Rep. Bobby Rush), www.energycommerce.house.gov.

8 *See* FTC Comment Form, www.ftcpublic.commentworks.com (calling for comments by January 31, 2011); Commerce Department Request for Comments, www.federalregister.gov (calling for comments by January 28, 2011).

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Steven C. Bennett
New York
+1.212.326.3795
scbennett@jonesday.com

Kevin D. Lyles
Columbus
+1.614.281.3821
kdlyles@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com