BNA Insights

TARGETED ADVERTISING

The Federal Trade Commission's proposed ''Do Not Track'' system, posted for public comment through Feb. 18, has the potential to dramatically expand the scope of consumer privacy rights at the expense of business interests. Although the name suggests similarities to ''Do Not Call'' or the industry-administered ''Do Not Mail,'' it could reposition the boundaries between personal privacy, on the one hand—and commercial property and speech rights on the other—ultimately jeopardizing the availability of free online content and harming the very consumers the proposal seeks to protect.

Marketing

Will The FTC's 'Do Not Track' Proposal Spell the End of Free Internet Content?

BY DANIEL T. ROCKEY

The Federal Trade Commission's December 2010 report on consumer privacy in the internet age concludes that industry self-regulatory efforts have been inadequate. The report proposes, among other potential remedies, the implementation of a ''Do Not Track'' mechanism akin to the FTCs ''Do Not Call'' registry,[1] under which consumers may opt-out on a global basis from being tracked while browsing online.[2]

There is broad consensus that the FTC's Do Not Call registry, and similar industry administered Do Not Mail programs, have been largely successful in curbing perceived marketing abuses and providing appropriate options to consumers. But the Do Not Track mechanism envisioned by the FTC would dramatically expand the right to privacy in the United States and, more pragmatically, is likely to lead to undesired and potentially disruptive consequences.

These consequences, on balance, may harm the very consumers the FTC seeks to protect.

Important Differences From 'Do Not Call'

The FTC has chosen to label its proposal ''Do Not Track,'' evoking benign perceptions associated with its successful Do Not Call list. But this new proposal is actually very different from Do Not Call and Do Not Mail.

The proposed Do Not Track differs from those programs both in the harms it is intended to address and the balance it strikes between a consumer's right to privacy, on the one hand, and the rights of business interests to control the terms of access to their intellectual property and to engage in constitutionally protected commercial speech on the other.

Although I certainly do not attribute nefarious intent to the FTC in choosing the label ''Do Not Track''—it is catchy and, at least superficially, seems to aptly convey the concept behind the proposal—in my view, to equate ''Do Not Track'' with ''Do Not Call'' and ''Do Not Mail'' is to indulge in a facile and ill-suited analogy that obscures the significant differences in the intellectual underpinnings of the programs and their implications. Perhaps more importantly, the chosen title obscures the dramatic expansion of the right to privacy that the proposal can be expected to bring about.

The U.S. Right to Privacy: Intellectual Underpinnings

The concept of the right to privacy in the United States can be traced to Justice Louis Brandeis and his

[1] The Do Not Call registry was implemented as part of the FTC's Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), promulgated pursuant to its authority under the Telemarketing and Consumer Fraud and Abuse Act (15 U.S.C.A. § 6102).

[2] *Protecting Consumer Privacy in an Era of Rapid Change*, Dec. 2010, p. 63-69 (''FTC Report'').

Daniel Rockey is of counsel with Bullivant Houser Bailey PC, working in the firm's San Francisco office. He provides counseling and litigation services to technology and other companies in the areas of privacy and data security and intellectual property, including trademark, copyright, domain name, false advertising and unfair competition matters.

  ECLR ISSN 1098-5190

1890 Harvard Law Review article entitled ''The Right to Privacy.'' Later, in his dissent in the 1928 case of *Olmstead v. United States*, he described the right to privacy as ''the right to be left alone.''[3]

The concept of the right to be left alone has been the foundation for privacy jurisprudence in the United States ever since, from the contours of the Fourth Amendment right to be free from unreasonable government intrusion into one's private affairs; to the tort of invasion of privacy (i.e., the right to be free from intrusions upon seclusion); and the right to make decisions concerning fundamental issues such as contraception, procreation and marriage.

It also serves as a key underpinning for legislative efforts to regulate personal privacy and, in particular, the rights of individuals to be free from harm resulting from the misuse of their personal information.[4]

And, of course, the right to be left alone provides legal justification for the FTC's Do Not Call registry; the assumption being that consumers, having once committed to install telephone service in their homes, have little control over who ''enters'' their homes by way of that electronic portal.[5]

Thus, in upholding Do Not Call in *Mainstream Mktg. Servs. v. FTC*, 358 F. 3d 1228, 1238 (10th Cir. 2004), the court stressed ''the unique nature of the home and recognized that 'the State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society.' ''[6]

A similar rationale has been used to justify Do Not Mail programs, on the theory that the consumer would otherwise be powerless to stem the tide of ''junk'' mail that floods one's mailbox.[7] Just as consumers may restrict entrance to their homes through their front door, they may also be given the option of limiting the extent to which marketers may ''enter'' their homes by way of the telephone or the mailbox.[8] The individual's right to privacy generally ends, however, when she chooses to venture out where she may be easily observed or overheard, or chooses to disclose information to third parties.[9]

To be sure, the right to be left alone *has* been extended to embrace certain interactions beyond the boundaries of the home or one's physical body. Thus, the Supreme Court held that the protections of the Fourth Amendment apply to telephone conversations about which consumer's have a reasonable expectation of privacy.[10] And Congress has chosen to limit the disclosure of information conveyed to third parties in certain narrowly defined categories, such as personal health information,[11] financial information,[12] private education information,[13] cable subscriber or video rental information[14] and, under certain circumstances, stored electronic communications.[15]

However, the evolution of the right to privacy has, until recently, been limited to areas of extreme sensitivity, or contexts in which the individual has both a subjective, and objectively reasonable, expectation of confidentiality.[16]

Expanded Right to Be Left Alone

The concept of a Do Not Track mechanism would expand the right to be left alone still further, beyond the confines of one's home and beyond the limited areas found to involve such sensitivity or confidentiality that compelled disclosure is intolerable.

The FTC does not advocate any particular mechanism for implementing Do Not Track, but it makes clear that it envisions a ''universal choice mechanism'' that would ''signal whether or not the consumer wants to be tracked or receive targeted advertisements'' and ''enable consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.''[17] Implicit in this concept is the notion, perhaps because consumers generally ''surf'' the web from the ''privacy'' of their homes or offices, that consumers should be able to do so surreptitiously and without being observed.

However, with few exceptions, in order to be tracked online a consumer must make an affirmative decision to venture beyond the confines of her home by directing her browser to establish contact with a distant server and request that content residing on that server be made available for download and display on the consumer's computer.

The consumer does not physically travel anywhere, of course, but by directing the browser at a URL the

---

[3] 277 U.S. 438, 478-9 (1928).

[4] E.g., FCRA/FACTA (denial of benefits based on inaccurate information; prevention of identity theft); Graham-Leach Bliley (misuse of financial information); HIPAA (medical information); COPPA (harm to minors from collected information).

[5] P.L. 103–297, Telemarketing and Consumer Fraud and Abuse Prevention, House Rep. No. 103-20 (''An abusive practice under this legislation could also take the form of a sales strategy of unsolicited telephone calls by a telemarketer where a pattern of calls could be considered by reasonable consumers to be coercive of a consumer's right to privacy.'').

[6] *Quoting Frisby v. Schultz*, 487 U.S. 474, 484, 108 S.Ct. 2495, 101L.Ed. 2d 420 (1988).

[7] *Rowan v. United States Post Office Dep't*, 397 U.S. 728 (1970) (upholding right to ''exercise control over unwanted mail,'' because ''[t]o hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home.'').

[8] *Cf. FCC v. Pacifica Found.*, 438 U.S. 726 (1978) (''[I]n the privacy of the home . . . the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder.'').

[9] *See, e.g., Katz v. United States*, 389 U.S. 347 (1967) (''What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.''); *Smith v. Maryland*, 442 U.S. 735 (1979) (''a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.''); *United States v. Miller*, 425 U.S. 435 (1976) (''This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'').

[10] *Katz*, 389 U.S. at 353.

[11] 42 USC § 1320d-6 (HIPAA).

[12] 15 USC § 6802(b) (Graham Leach Bliley)

[13] 20 USC § 1232g(b)*Educational Rights and Privacy Act* (Family Educational Rights and Privacy Act).

[14] 18 U.S.C. § 2710(b) (Video Privacy Protection Act)

[15] 18 U.S.C. §§ 2701-2712 (Stored Communications Act)

[16] *United States v. Warshak, et al.*, 2010 WL 5071766 (6th Cir. December 14, 2010)(15 ECLR 1925, 12/22/10).

[17] FTC Report, at 66-8.

consumer is requesting access to content created and hosted by someone else and makes herself ''observable'' by the device hosting the content, by the content provider's partners, and by the internet service provider transmitting the request.

Whether the consumer is ''visiting'' the virtual storefront of a retail business, searching the files of an academic institution or government agency, or interacting within a social networking community, there seems to be little qualitative difference between browsing the virtual ''aisles'' of a website and strolling down the actual aisles of its brick and mortar equivalent. Just as a brick and mortar site incurs substantial operating costs and has an obvious interest in understanding who is visiting it, an internet content provider often generates that content at great effort and expense and has arguably an equal interest in controlling access to that content and understanding who is ''visiting'' the site.

Few would argue, however, that an individual who enters a brick and mortar location should have the legal right to prohibit the owner from observing them, monitoring their movements within the building, or offering purchase suggestions.

Internet Exceptionalism at Work?

Yet, in what appears to be a textbook example of what Santa Clara University Law Professor and noted internet scholar Eric Goldman refers to as internet exceptionalism—that is, the tendency to treat situations presented by the internet differently from the real-life contexts which they resemble; as if they were *sui generis*—the FTC posits that consumers should be able to venture onto the internet, and enter the virtual confines of commercial establishments, while preserving their anonymity and with the ability to prevent those commercial establishments or their marketing partners from observing them.[18]

In effect, Do Not Track would expand the right to be left alone well beyond the confines of one's home to anywhere the consumer wishes to travel within the virtual world of the internet. And while there does appear to be a qualitative difference between physically venturing beyond your front door and venturing onto the internet, analogizing Do Not Track to Do Not Call and Do Not Mail obscures these differences and leads the FTC to propose a substantial expansion of personal privacy beyond prior constitutional notions without fully acknowledging this expansion or its potential repercussions.

Two recent appellate decisions help to illustrate how the FTC's Do Not Track proposal may well raise serious constitutional issues.

In *Sorrell v. IMS Health Inc.*, 2010 WL 4723183 (2d Cir. Nov. 23, 2010) (15 ECLR 1807, 12/8/10) (*petition for certiorari granted* Jan. 7, 2011) (16 ECLR 62, 1/12/11), the Second Circuit U.S. Court of Appeals held that a Vermont law prohibiting pharmacies from sharing prescriber information with pharmaceutical companies for data mining and marketing purposes was an unconstitutional restriction on commercial speech.

The court found the law unconstitutionally restrictive even though it did not create an outright ban on the sharing of prescribing information, and instead merely provided doctors the ability to opt-out of having that information shared for marketing purposes.[19] Although the Supreme Court recently granted review of the decision—and could well overturn it—the decision raises serious questions as to whether a rule prohibiting internet content providers or network advertisers from sharing data gathered from visitors to their sites, or using it for marketing purposes, would pass constitutional muster.[20]

In another recent decision, *United States v. Warshak, et al.*, 2010 WL 5071766 (6th Cir. December 14, 2010) (15 ECLR 1925, 12/22/10), the U.S. Court of Appeals for the Sixth Circuit held for the first time that the protections of the Fourth Amendment apply to e-mail.

In so holding, the court explained that the question of whether communications are protected by the Fourth Amendment involves two questions: Whether the individual has a subjective expectation of privacy in the communication; and whether society is willing to recognize that expectation as reasonable?[21]

Comparing e-mail to letters and telephone communications, which the court previously held to be subject to Fourth Amendment protection, the court determined that both inquiries were satisfied with respect to e-mail communications.[22] This was true notwithstanding the fact that an individual's ISP might have the ability, even the contractual right, to access the individual's email for certain purposes.[23]

Although the FTC's Do Not Track proposal would not instantly render web surfing activity subject to Fourth Amendment protections, it is reasonable to ask whether creating a special, state-mandated ''zone of confidentiality'' around internet activity might have unintended implications on the development of Fourth Amendment jurisprudence in the area of the internet and, theoretically, might even impact the government's ability to track terrorist activities online.

Although the FTC laudably solicits public input on various technical and policy issues concerning Do Not Track, notably absent from the FTC's Report is any meaningful acknowledgement or reflection on the expansion of the right to privacy which Do Not Track represents, or the potential constitutional implications of enacting the FTC's proposal.[24]

Boundary Shift Undermines the Implicit Bargain That Drives the Internet

Some may dismiss the foregoing discussion as little more than an interesting academic exercise. But this attempt to reposition the boundaries between personal privacy—and commercial property rights and commer-

[18] For fans of the *Harry Potter* series, a virtual invisibility cloak, if you will.

[19] *Id.* at *14-5.

[20] *IMS Health Inc. v. Sorrell*, 2010 WL 4723183 (2d. Cir. 2010) *cert. granted*, *Sorrell v. IMS Health Inc.*, ___ S.Ct. ___, 2011 WL 48123, 79 USLW 3370 (U.S. Jan. 7, 2011) (holding that ban on pharmacies sharing prescriber information with data mining companies was impermissible restraint on commercial speech).

[21] *Id.* at *9.

[22] *Id.* at *11-12.

[23] *Id.* at *12.

[24] *But see* Concurring Statement of Commissioner J. Thomas Rosch (questioning constitutionality of ban on tracking), at E-6.

   ISSN 1098-5190

cial speech—also undermines the implicit bargain which drives the internet and makes available to consumers vast amounts of information, seamlessly and without out-of-pocket cost to the consumer.

As the internet has matured, there has developed an implicit exchange of value between consumers and content providers. In essence, the content provider agrees to make content available to the consumer in exchange for the consumer's agreement to submit to display or other ads. Thus, the content provider ''sells'' the consumer content, and the consumer ''purchases'' content by giving the provider, or more often, a marketing partner such as a network advertiser, the opportunity to present them with an advertisement and the opportunity to convince them to purchase something. The content provider generates ad revenues to pay for the generation of content, and the consumer gets to do what it does best—consume.

Furthermore, although the data is somewhat anecdotal at this point, a consensus seems to be emerging that in order for this implicit bargain to generate sufficient revenue to support the creation of rich content—e.g., in the case of news organizations, or other organizations for which content creation and renewal is costly and labor intensive—so-called ''run-of-network'' or non-targeted ads may not generate sufficient revenue to ensure the continued supply of content.

A recent study lead by former Director of the FTC's Consumer Protection Bureau, Howard Beales, found that behaviorally-targeted advertising is more than twice as effective at converting users who click on ads into buyers (6.8 percent conversion vs. 2.8 percent for run-of-network ads) and that the weighted average cost per thousand ad impressions (CPM) for behaviorally targeted ads was $4.12, as opposed to $1.98 for run-of-network advertising.[25] The study further found that more than half of the revenue generated by network advertisers went towards the purchase of inventory and was therefore shared with publishers and content providers to support their businesses. Although causation is obviously difficult to establish in this context, it is evident that the growth in targeted advertising online has coincided with dramatic growth in the availability, depth and variety of ''free'' content and services on the internet.

The FTC's proposal to compel the creation of a Do Not Track mechanism that would permit, if not encourage, consumers to opt out globally of all online tracking threatens to put an end to this Golden Age of ad-supported Internet content and services.[26]

Indeed, by advocating a system under which consumers may prohibit content and service providers from using targeted advertising, the FTC is creating what is from an economic point of view a classic ''free-rider'' problem. In effect, the FTC is endorsing the notion that consumers may reap the enormous benefits in terms of content, access and services that the internet has to offer while denying providers the ability to serve ads targeted to the presumed interests of their users; essentially encouraging consumers to acquire benefits for ''free.''[27]

Although no one knows for certain what the impact of a Do Not Track mechanism with a high utilization rate would be, it seems highly likely that as more and more people opt out of targeted advertising—effectively cutting potential revenue streams in half, if the Beales study is accurate—that the quality of ad-supported content and services will suffer dramatically.

Now, no one would argue against transparency or providing consumers with choice, and the ability to control what they choose to share. And, as the FTC recognizes, if consumers understand the implicit bargain, and the benefits associated with targeting—e.g., less obnoxious ads, and ads that are much more likely to be of interest to the consumer—they may well choose to share certain information in exchange for those benefits. But while each individual may understand the benefits, there is a significant risk—illustrated by the widely accepted economic concept of the ''tragedy of the commons''[28]—that if the scales are tipped in favor of opting out there is reason to believe that consumers will choose to free-ride and that free content may soon be a thing of the past.

Conclusion: Explore the Possibilities

Although many of my clients in the online marketing field remain highly skeptical of Do Not Track, the purpose of this article is neither to undermine Do Not Track or discourage the FTC's very laudable exploration of ways in which to provide consumers with more choices and more control.

The purpose is simply to ensure that all engaged in this effort appreciate the rather radical proposition that Do Not Track represents, and carefully consider the myriad potentially harmful implications that may flow from the government interceding in the marketplace to compel adoption of a Do Not Track mechanism. In light of recent announcements by the three major browser developers (Microsoft, Google and Mozilla) that they will incorporate anti-tracking technologies into upcoming versions of their browsers—on top of existing industry efforts to provide opt-out choices for consumers—it is reasonable to ask whether the FTC's premise that self-regulatory efforts have been inadequate is sound. And it is reasonable to ask, in light of the potential constitutional implications, and the uncertain impact that FTC intervention might have on the vitality of the internet, whether now is the time for the FTC to intercede and begin redefining the right to privacy; or whether consumers would in fact be better served by the FTC maintaining its ''wait and see'' approach to this very complex and thorny issue.

---

[25] The Study can be found at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[26] Indeed, there are indications that even with targeted advertising, ad-supported content may already be imperiled. See, e.g., ''The Times to Charge for Frequent Access to Its Web Site,'' http://www.nytimes.com/2010/01/21/business/media/21times.html.

[27] Although we should not mistake the FTC's endorsement of a Do Not Track mechanism with advocating that consumers actually use that mechanism to opt-out, the FTC's report comes awfully close to the latter by pointing to low click through rates as evidence that self-regulatory efforts have been ineffective and seemingly equating low-opt out rates with a lack of consumer awareness. FTC Report, p. 64-5.

[28] The principle of the ''tragedy of the commons'' is generally traced to Garrett Hardin in his now famous article in Science magazine, in 1968, in which he posited that where a valuable resource is subject to unrestricted, use by all it will become overused and eventually destroyed.