Antitrust, Vol. 31, No. 3, Summer 2017.

Tracking the Past and Future of Interest-Based Advertising

BY MEREDITH HALAMA AND MICHAEL SHERLING

FOR ALMOST AS LONG AS AMERICANS have looked to the Internet for news, weather, sports scores, and other valuable and entertaining information, online advertising has fueled the availability of such content. Initially, ads were customized—if at all—only on the basis of the site the user was viewing. Advertisers had little insight into how effective their ads were or how users interacted with them.

In the mid-1990s, however, new business models emerged that enabled data to be collected and correlated across nonaffiliated websites, giving advertisers the ability to optimize their campaigns and to understand how users interact with them. This data—bits of information left behind by consumers navigating the web, often referred to as "clickstream data"—also enabled advertisers to target their campaigns to people who were most likely to be interested in them—whether that meant sports enthusiasts, men living in Los Angeles that fell into a certain age range, or people in the market for a new car. This "network advertising" also allowed publishers to earn greater revenues from the ads served on their sites because users were more likely to act on them.

At the same time, these business models enabled the collection of vast swaths of web browsing behavior in ways that were largely invisible to consumers, causing concern among regulators and privacy advocates. Online behavioral advertising (today referred to as "interest-based advertising") has only grown more complex in the intervening years. With that complexity, calls for regulatory action and simplified choice mechanisms have at times reached frenzied heights.

In this article, we take the advent of a new administration as an opportunity to look back on the policymaking and enforcement treatment of online advertising and to consider what the coming years may hold for the online advertising industry and the publishers and advertisers that depend on it.

Meredith Halama and Michael Sherling are attorneys in the Washington, DC office of Perkins Coie LLP. Meredith Halama is a Partner in the Privacy and Security subgroup of the firm's Commercial Litigation practice. Michael Sherling is an associate in the Technology Transactions & Privacy Law group.

The Mid-1990s: Online Profiling and Early Industry Response

Between 1996 and 1999, the commercial Internet grew exponentially. With this growth came regulatory concerns around the privacy of Internet users. In a series of reports to Congress in the late '90s and again in 2000, the Federal Trade Commission identified widely accepted principles regarding the collection, use, and dissemination of personal information known as the fair information practice principles (FIPPs) as applied to the practices of commercial websites, eventually calling on Congress to pass comprehensive privacy legislation.[1]

In parallel with this increased general concern about privacy online, the FTC scrutinized the collection of data for online advertising purposes in particular. In 1999, the FTC held its first workshop focused on online advertising. The same year, DoubleClick, one of the most successful early ad networks, acquired Abacus, a data broker that collected information about individuals' offline activities. DoubleClick, like other early ad networks, relied on cookies to identify unique browsers and generally did not collect or use individuals' names, email addresses, or other personal information to target ads to them. To that end, it had publicly committed not to combine users' clickstream data with data that identified them personally.

With the purchase of Abacus, advocates questioned whether DoubleClick would honor these commitments and called on the FTC to investigate DoubleClick's practices. In response, the FTC launched an investigation to determine whether DoubleClick had engaged in deceptive trade practices by collecting, using, and disclosing consumer information in violation of Section 5 of the FTC Act. The FTC focused in particular on whether DoubleClick used or disclosed consumers' personal information in contravention of its privacy promises by combining clickstream data with personal information, and whether it used sensitive information in contravention of its privacy policy. The FTC eventually closed this investigation, finding that DoubleClick had not breached its privacy representations and highlighting DoubleClick's participation in self-regulatory efforts as essential to its decision.[2]

Amid FTC scrutiny and calls for legislation, DoubleClick and other major online advertising companies attempted to demonstrate to the FTC that industry could be trusted to regulate itself. To that end, a coalition of the leading network advertisers (at the time, fewer than 10 companies) formed the Network Advertising Initiative (NAI) in order to develop a framework for self-regulation of the online profiling industry. The NAI is a membership organization comprised entirely of ad networks and other "third parties," and would become a central player in efforts to implement and enforce privacy protections with respect to online advertising.

Though the NAI's principles have evolved over the years, they have always required, in essence, participating companies to: (1) provide notice to users that explains their data collection practices in their privacy policies and to make reasonable efforts to ensure that notice is provided on the websites and apps where they collect data used to target ads to consumers; (2) offer consumers choice with respect to online profiling; and (3) employ security protections with respect to the data they collect. Notably, responding to the concerns expressed in the DoubleClick-Abacus merger, the NAI Principles also restricted (and continue to restrict) the use of personal information, such as name, email address, phone number, or physical address for online advertising, incentivizing NAI member companies to rely only on cookies and other forms of device identifiers to track browsing activity. The NAI also restricts the use of information about health-related interests and other sensitive data for purposes of selecting what ad to show a consumer.

A New Century: FTC Policy Efforts Around Online Tracking

Report to Congress. The FTC issued its first report on what it then called "online profiling" to Congress in the summer of 2000. Following a formula to which it would return many times in its discussion of online advertising in subsequent years, the FTC noted the benefits of targeted ads to consumers, advertisers, and publishers, but also noted privacy concerns, including the hidden nature of network advertisers' activities, and the "extensive and sustained scope of the monitoring that occurs."[3] The FTC observed that much online advertising relies on non-identifying information such as identifiers stored in cookies,[4] but that for many, "the privacy implications of profiling are not ameliorated in cases where the profile contains no personally identifiable information."[5]

In its report, the FTC commended the NAI Principles but also recommended "backstop legislation addressing online profiling," noting the need to address "recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program" and that only legislation could guarantee that notice and choice are always provided when and where consumers needed such information.[6] While the FTC later backed away from calls for legislation specific to the online advertising industry, it would cite similar concerns when calling for a comprehensive Do Not Track technical solution as discussed below.

This early report and the conclusion of the DoubleClick investigation left the online advertising industry with baseline rules that would guide it for more than a decade: (1) offer consumers notice and choice with respect to online profiling; (2) be wary of the use of PII in online tracking; and (3) hew closely to self-regulatory principles to help avoid legislation that could severely limit the ability to profile users and serve targeted ads. Against this backdrop, the dot.com bubble promptly burst, driving out of business many of the network advertising companies that had formed the NAI and placing privacy concerns around online tracking on the backburner.

2007–2009: Renewed Interest in Online Advertising and Reinvigorated New Self-Regulation. By 2007, online advertising had reemerged as a powerful market force. Spurred by renewed investment in Internet advertising, in 2009 the FTC released a report setting forth four recommendations or "principles" for online behavioral advertising: (1) provide notice of data collection practices and choice with respect to behavioral advertising on every website where data is collected for behavioral advertising purposes; (2) implement reasonable security and data retention practices for data collected for online advertising purposes; (3) obtain affirmative express consent from affected consumers before using previously collected data in a manner that is materially different from promises made when the data was collected; and (4) obtain affirmative express consent before using sensitive data—e.g., data about children, health, or finances—for behavioral advertising.[7]

Several themes emerged in the 2009 Report that would reappear in FTC policy guidance and enforcement actions over the following years. For example, the FTC underscored the importance of notice and choice where data is collected (a theme that it later termed "just in time" notice), and the need for "a clear, easy-to-use, and accessible method" for users to express choice with respect to such practices. The FTC also emphasized the need for privacy protections even for data that does not identify users personally, as its framework applied not only to data associated with an identified individual but also to any data that could reasonably be associated with a particular computer or other device. The FTC later expanded this approach to commercial privacy generally in its seminal 2012 Privacy Report.

The 2009 Report also shows FTC Staff distinguishing, for the first time, between "first party" and "third-party" practices. "First parties" are generally considered those entities with which the consumer directly interacts, while "third parties" are those entities that collect data without the consumer's knowledge or knowing interaction. The 2009 Report proposed exempting from the Principles "first party" and "contextual" behavioral advertising models under the theory that such practices are more likely to be within the scope of consumers' expectations and less privacy-invasive than

models involving ongoing tracking of consumer movements online. The FTC would continue this line of thinking over the next several years, drawing policy distinctions between companies with which users directly interact and those that collect data in the background.

Finally, the 2009 Report put industry on notice that the FTC would be watching it closely, noting that staff would "conduct investigations, where appropriate, of practices in the industry to determine if they violate Section 5 of the FTC Act or other laws."[8] As we discuss below, the FTC would remain true to its word.

As the FTC renewed its focus on online advertising between 2007 and 2009, the online advertising industry redoubled its self-regulatory efforts in an attempt to stave off government regulation. For example, in 2008 the NAI—now composed of dozens of companies engaged in online behavioral advertising—updated its Principles to contain more rigorous restrictions on the collection and use of sensitive data and to provide for public reporting of violations of the NAI Principles by member companies. The following year, responding to calls from the FTC to involve all parts of the online advertising ecosystem in self-regulatory efforts, a coalition of industry groups (later named the Digital Advertising Alliance or DAA) adopted a set of Self-Regulatory Principles for Online Behavioral Advertising. The DAA, unlike the NAI, imposes obligations on all players in the online advertising ecosystem—including advertisers, publishers, and the "third-party" online advertising companies. Responding to FTC calls for independent enforcement of self-regulatory rules, the DAA empowered the Council of Better Business Bureaus to bring public enforcement actions against non-compliant companies.

To the consternation of many privacy advocates and regulators, however, both the NAI and DAA adopted opt-out mechanisms that allow data collection to continue even when a user has opted out and which could be inadvertently deleted by users. These mechanisms work by allowing consumers to set opt-out cookies on their browsers that signal to participating companies that they do not wish to receive targeted ads. These "opt-out cookies" do not stop data collection, and indeed the self-regulatory rules explicitly permit companies to continue collecting data for purposes other than serving interest-based ads even after consumers have opted out. Because these opt outs are cookie-based, moreover, they disappear whenever users clear their browsing history, leading many to criticize them for their fragility. The perceived weakness of these choice mechanisms would prompt calls for browser-based choice mechanisms that would limit data collection and that could not be inadvertently overridden.

2010–2012: Comprehensive Evaluation of Consumer Privacy. Between 2010 and 2012, FTC Staff undertook a comprehensive analysis of consumer privacy, first issuing a preliminary staff report,[9] and ultimately its influential 2012 Privacy Report, giving it another opportunity to evaluate online behavioral advertising practices, now in the context of general consumer privacy issues.[10] In its preliminary report, FTC Staff expressed frustration with industry's progress in providing consumers the ability to control how data is collected and used for behavioral advertising purposes in a uniform manner, observing that industry had failed to implement an effective choice mechanism on an industry-wide basis, that consumers were unaware of the choice mechanisms provided by industry, and that consumers did not understand the effect of the choices they did make.[11]

While industry devoted substantial energy toward implementing a Do Not Track system, efforts to adopt an industry-wide technical standard fell apart in 2013, in no small measure due to disputes over the proper treatment of first-party and third-party tracking.

Given these perceived privacy shortfalls, FTC Staff expressed support for a more uniform and comprehensive choice framework for online behavioral advertising through a browser setting known as "Do Not Track." Such a setting would, staff reasoned, prevent consumers from needing to opt out on a company-by-company or industry-by-industry basis, would ensure that users' choices would not disappear when the user cleared cookies, and would address concerns about existing choice mechanisms by "being more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking."[12]

Two years later, in its final Privacy Report, the FTC doubled down on Do Not Track, calling on industry to continue to work to complete implementation of an easy to use, persistent, and effective Do Not Track system. As it had done in its 2009 Online Behavioral Advertising Report, the FTC excluded first-party and contextual advertising from its calls for transparency and simplified choice, reasoning that no special protections are necessary for practices that "are consistent with the context of the transaction" or with "the company's relationship with the consumer."[13] While industry devoted substantial energy toward implementing a Do Not Track system, efforts to adopt an industry-wide technical standard fell apart in 2013, in no small measure due to disputes over the proper treatment of first-party and third-party tracking.[14]

2015–2017: Cross-Device Tracking. As consumers' eyeballs have shifted from the web to smartphones, tablets, and mobile apps, online advertising companies have developed mechanisms to track them across those devices using a variety of methods. These methods include both deterministic methods and probabilistic models. Deterministic methods are based on consumers logging in and using the same credentials or otherwise submitting the same personal information on different devices, allowing companies to

see that the same person owns different devices. Probabilistic models use data from different devices to make educated guesses that different devices belong to the same person.

In its 2017 report on cross-device tracking, the FTC noted the benefits of cross-device tracking, including more relevant ads, but also privacy concerns, including the ubiquity of data collection, much of which is largely invisible to consumers, a lack of notice and transparency for consumers about whether the practice is occurring and its scope, and the difficulty consumers have in opting out of tracking across devices.[15] In light of these concerns, the report made several recommendations. First, companies implementing cross-device tracking should be explicit that consumers are being tracked across their devices. Second, companies should implement choice mechanisms that give consumers control over how their data is collected and used across platforms. And finally, companies should refrain from tracking consumers and serving ads based on sensitive information, including health, financial, and children's information.[16] The FTC did not, however, require companies to deem an opt out made on one device as applying to all other devices that the company had associated with a user, noting the technical difficulties with implementing a single opt out.

Kids and Online Tracking: An Expanded Definition of Personal Data

Advertising to children has always attracted special scrutiny from the FTC. The Children's Online Privacy Protection Act (COPPA) gives the FTC rulemaking authority (and the ability to impose statutory penalties) with respect to the collection of data from children known to be under 13 and on websites and online services directed to children—authority it generally otherwise lacks with respect to online tracking.

In 2013, the FTC used that rulemaking authority to explicitly address online tracking of children in updating its COPPA Rule. Most controversially to the online advertising ecosystem, that rule expanded the definition of "personal information" to include not only "traditional" personal information, such as name, email address, physical address, and phone number, but also "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services,"[17] including "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[18] Where persistent identifiers are used only to "support the internal operations of the web site or online service" and the operator collects no other personal information, the operator is not obligated to provide notice or to obtain verifiable parental consent as defined by COPPA. But where such identifiers are used for "behavioral advertising, or to amass a profile on a specific individual, or for any other purpose," an operator must provide notice and obtain verifiable parental consent to use or disclose such identifiers. Moreover, ad networks and other third-party companies are deemed "operators" as defined by COPPA when they know that the site or service from which they are collecting data is directed to children, such that they can be held accountable for violations of COPPA even where they are not providing child-directed content.[19]

Although COPPA is limited to tracking users whom the operator knows to be under 13 and to tracking on sites and services directed to children, these updates to the COPPA Rule were viewed by many observers as a shot across the bow to the online advertising industry. While the years of policy guidance outlined above had always made clear that data tied to a device, but not reasonably tied to an individual, was *entitled to privacy protections* such as notice and choice, the 2013 update to the COPPA Rule was the first time the FTC suggested that such data was entitled to *the same level* of privacy protection as data that directly identifies an individual. Then-Director of Consumer Protection Jessica Rich would later underscore this position, asserting that the FTC views cookies and similar identifiers not only as worth of privacy protections but as "personal information" even outside of COPPA.[20]

Given its lack of rulemaking authority outside of sites and services that are directed to children, the scope of the FTC's authority to act on such an expansive definition of personal information is not clear. Nevertheless, companies are on notice that they can no longer blithely assert that the cookies and similar identifiers they use to track users are not personally identifiable.

Snapshot of FTC Enforcement Actions on Online Tracking

Between 2010 and 2016, the FTC made good on its 2009 promise to closely monitor the online advertising ecosystem and bring enforcement actions where it perceived a violation of Section 5. These actions represent several major themes: (1) that offering a choice that does not work as represented is a deceptive practice, regardless of how many users actually avail themselves of such choices; (2) that the FTC views with suspicion comprehensive tracking of every movement a consumer makes online, and holds companies to high notice and consent obligations for those practices; (3) that the FTC will hold tracking companies accountable for the failure to make notice available that consumers are being tracked; and (4) that the FTC will use its COPPA authority broadly to prevent online tracking of kids and on sites and services directed to children.

Providing Illusive Choice Mechanisms. While lacking rulemaking authority to require online advertising companies to offer any particular form of choice for online tracking (save, of course, for under COPPA), the FTC has brought several cases designed to send the message that whatever choice mechanism the company offers or describes, the failure of that choice mechanism to work as described is a deceptive practice. For instance, *Chitika, Inc.* concerned an ad network that offered the ability to opt out by setting an opt-out cookie on the user's browser. This opt out, however, lasted

only 10 days. The FTC charged that Chitika, in offering consumers the ability to opt out, implicitly or explicitly represented that its opt out would last for a "reasonable" period of time, such that its failure to provide an opt out that lasted for a reasonable period of time was deceptive.[21]

The FTC has also brought three cases against companies that represented that blocking cookies would stop tracking when, in fact, it did not. The first concerned ScanScount, Inc., an ad network that used flash cookies to track users even when they blocked cookies from being accepted by their browsers.[22] The second concerned Google's publication of help center content informing Safari users that they need not opt out of online tracking if they used Safari with its default settings because that browser blocked third-party cookies. In fact, due to a technical implementation, Google tracked users employing Safari's default settings for a short period of time.[23] The third involved Turn Inc.'s use of code transmitted from the devices of Verizon subscribers to uniquely identify those devices, even when cookies were blocked. This practice, in the FTC's view, rendered Turn's representations regarding the effect of blocking cookies to be deceptive.[24] The FTC also found that language in Turn's opt-out page deceptively suggested that opting out would affect targeting in mobile apps, when in fact it only affected targeting on websites.

More recently, the FTC alleged that InMobi Pte Ltd. misrepresented choices users had with respect to location-based tracking. InMobi, a company that enables app developers to serve ads in their apps, including ads based on users' locations, stated that it only tracked consumers' locations after they opted in and that its software would abide by device privacy settings. In reality, InMobi tracked consumers' locations using a variety of technologies even when consumers did not allow apps to access to their location via their devices' GPS-based location setting.[25] This tracking, in the FTC's view, rendered InMobi's representations about the effect of consumers' choices to be deceptive.

Comprehensive Tracking. Through its policy-related initiatives, the FTC has expressed skepticism of companies that engage in comprehensive tracking of every website—or nearly every website—a user visits.[26] Its enforcement actions reflect that skepticism, finding violations of Section 5 where companies fail to provide sufficient information about those practices to allow consumers to make educated decisions about the choices available to them. For instance, the FTC charged that Epic Marketplace, Inc.'s failure to disclose its use of "history sniffing" code that can detect whether a consumer had visited hundreds of thousands of websites, regardless of whether those sites participated in the Epic Marketplace network, was a material omission because it would have been relevant to users' decision of whether to opt out.[27]

In a case brought against Sears, the FTC found that Sears engaged in a material omission when it tracked nearly every website a user visited and every action they took online via an application users could download in exchange for $10 and the opportunity to participate in a Sears user panel. Notably, the End User License Agreement (EULA) used for this program did disclose that once the application was installed it would monitor "all of the Internet behavior that occurs on the computer on which you install the application, including both your normal web browsing and the activity that you undertake during secure sessions, such as filling a shopping basket, completing an application form or checking your online accounts, which may include personal financial or health information." This disclosure, however, was buried deep within the agreement. From this, the FTC concluded that Sears failed to adequately disclose that the application would monitor nearly all internet behavior, a fact that would be material to consumers in deciding whether to install the application.[28]

Meaningful Notice and Choice. Through its online advertising reports, the FTC has made clear that notice should be provided to consumers where data is collected about them, a theme that shows up in the FTC's enforcement actions as well. For instance, the FTC faulted Nomi Technologies, Inc. for not providing notice to consumers that it was engaged in tracking consumers' cell phones in retail stores despite an implied promise to do so. In its privacy policy, Nomi pledged to "[a]lways allow consumers to opt out of Nomi's service on its website *as well as at any retailer using Nomi's technology*."[29] The FTC reasoned that this statement constituted an implicit or explicit promise that consumers would be given notice that they were being tracked by Nomi when they were in retail stores that integrated Nomi's technology and that they could opt out while in retail stores. In reality, neither Nomi nor its retail customers informed consumers that they were being tracked while in the retail stores.

A similar theme emerged in an action against InMobi Pte Ltd. There, the FTC pointed not only to representations InMobi had made to consumers, but also to misrepresentations it had made to developers that integrated its software development kit (SDK) about how its location tracking worked.[30] As a result of these misrepresentations, the FTC reasoned, "[a]pplication developers could not provide accurate information to consumers regarding their applications' privacy practices" and consumers were deprived of the "ability to make informed decisions about their location privacy and to control the collection and use of their location information through the thousands of applications that have integrated the InMobi SDK."[31] In other words, the FTC will demand that companies engaged in online and mobile tracking not only make accurate statements, but also that they enable the companies that integrate their technologies to make accurate statements and to provide meaningful choice to consumers.

Tracking Kids on Child-Directed Sites and Services. At the end of 2015, the FTC brought its first two enforcement actions under its recently-updated COPPA Rule. In both complaints, Retro Dreamer and LAI Systems, LLC, the

[T]he online advertising industry will have its regulatory hands full for the foreseeable future as it contends with the European Union's forthcoming General Data Protection Regulation (GDPR) and ePrivacy Regulation. These regulations are expected to impose massive regulatory burdens on online tracking, including proscriptive notice and choice requirements, access rights, and the "right to be forgotten."

FTC alleged that these developers of child-directed apps allowed interest-based ads to be served in their apps and allowed third-party advertising networks to collect personal information in the form of persistent identifiers.[32] InMobi similarly faced COPPA allegations relating to its collection of personal information in the form of device identifiers and location information from applications whose developers had informed InMobi were directed to children. These early cases, though presenting obvious COPPA infractions, demonstrate that the Commission is serious about stopping profiling and targeted ads with respect to children.

2017 and Beyond: The Future of Online Advertising and the FTC

Many observers expect the election of Donald Trump to result in a substantial shift in the FTC's consumer protection priorities. That shift may well disproportionately affect the online advertising industry.

In a speech given shortly after she was tapped to lead the Commission, Acting Chairman Ohlhausen invoked her dissent in *Nomi* to announce that the agency would not pursue enforcement actions where there was not a clear indication of consumer harm.[33] The *Nomi* dissent gives us a glimpse into how a Republican-led Commission might evaluate a case involving invisible tracking of consumers in a manner that breaks from the prior administration. In *Nomi*, then-Commissioner Ohlhausen found that the fact that Nomi made a statement that was technically inaccurate or misleading—that consumers could opt out while in the retail stores where Nomi's technology was used—was insufficient to find a violation of Section 5 that warranted use of the Commission's limited resources. She argued in dissent that "the Commission should use its limited resources to pursue cases that involve consumer harm" and that it "should not apply a de facto strict liability approach to a young company that attempted to go above and beyond its legal obligation to protect consumers but, in so doing, erred without benefiting itself."

To the extent the Commission acts on this vision, focusing its limited resources on cases that involve consumer harm, the online tracking industry might expect decreased FTC scrutiny in the coming years. Despite a nearly 20-year focus on online advertising by the FTC, evidence of concrete consumer harm is scarce. Rather, the FTC has sought to protect consumers' dignitary interests—interests, for example, in understanding when they are being tracked and in having the choice to avoid having their online activities monitored. Skeptics of the online advertising industry, including former Director of the Bureau of Consumer Protection David Vladeck, have repeatedly voiced concern that consumers' browsing habits will be used to deny them crucial benefits. An often-invoked hypothetical is a consumer browsing the Internet for a deep fat fryer that is "read as a telltale signal of an unhealthy habit" by a health insurer or potential employer.[34] But while such hypothetical use cases are often invoked as a reason for FTC intervention or legislation, to date neither the FTC nor consumer advocates have produced evidence of such misuse in any enforcement action or policy report.

But even without findings of harm, industry may not get off that easy. In the United States, despite rhetoric around the importance of focusing on concrete harm, a review of the FTC's cases involving online tracking demonstrates that commissioners from both parties have been willing to vote out cases where no concrete consumer harm was alleged. And even Acting Chairman Ohlhausen has emphasized that the misuse of "ubiquitous data collection and big data technologies" may create concrete privacy harms, and has noted that a notice-and-choice approach to privacy may not adequately protect consumers from tracking by companies that assemble bits of non-sensitive consumer information into a potentially sensitive mosaic of a consumer. Given these concerns, we may continue to see the FTC bring enforcement actions where companies make obvious misrepresentations, even where any possible concrete harm from such statements is speculative.

Outside of the United States, the online advertising industry will have its regulatory hands full for the foreseeable future as it contends with the European Union's forthcoming General Data Protection Regulation (GDPR) and ePrivacy Regulation. These regulations are expected to impose massive regulatory burdens on online tracking, including proscriptive notice and choice requirements, access rights, and the "right to be forgotten." Regardless of how companies ultimately respond to these requirements, whether by avoiding the EU, by developing unique solutions for EU consumers, or by building single global compliance mechanisms, these laws are certain to impact online tracking practices, and may force industry back to the table on Do Not Track. EU regulators, moreover, may respond to any perceived reduction in regulatory pressure on the online advertising industry in the United States by focusing additional attention on online and mobile tracking. Whatever path industry and regulators take, it is a safe bet that any regulatory break industry receives from the FTC will be more than filled by regulators in the EU. ■

[1] *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

[2] *See* Letter from FTC to Counsel for DoubleClick, Inc. (June 22, 2001), https://www.ftc.gov/sites/default/files/documents/closing_letters/doubleclick-inc./doubleclick.pdf.

[3] FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS PART I, at 12 (June 2000) [hereinafter ONLINE PROFILING REPORT PART I], https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf; FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS PART II, at 9 (July 2000) [hereinafter ONLINE PROFILING REPORT PART II].

[4] ONLINE PROFILING REPORT PART I, *supra* note 3, at 4.

[5] *Id.* at 12.

[6] ONLINE PROFILING REPORT PART II, *supra* note 3, at 10.

[7] FEDERAL TRADE COMMISSION, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009) (staff report), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[8] *Id.* at 48.

[9] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010) (staff report) [hereinafter Preliminary Privacy Report], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

[10] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012) [hereinafter 2012 Privacy Report], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[11] *Id.* at 65.

[12] *Id.* at 65–66.

[13] *Id.* at 48.

[14] Brian Fung, *The Internet's Best Hope for a Do Not Track Standard Is Falling Apart. Here's Why*, WASH. POST, Oct. 11, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/11/the-internets-best-hope-for-a-do-not-track-standard-is-falling-apart-heres-why/?utm_term=.d78a4ca70d15.

[15] FEDERAL TRADE COMMISSION, CROSS-DEVICE TRACKING (Jan. 2017) (staff report), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

[16] *Id.* at 15–16.

[17] 16 C.F.R. § 312.2 (2013).

[18] *Id.*

[19] *Id.* COPPA protections apply to "operators" of websites that collect or maintain personal information and which collect or maintain personal information from or about the users of or visitors to such Web sites or online services. In its commentary accompanying the final Rule, the Commission noted that the Rule covers an ad network when it has actual knowledge that it is collecting personal information through a child-directed Web site or online service. Statement of Basis and Purpose, Final Amendments to Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3972 (Jan. 17, 2013).

[20] Jessica Rich, Director of the Bureau of Consumer Protection, *Keeping Up with the Online Advertising Industry*, FTC BUSINESS BLOG (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[21] *See* Chitika, Inc., 151 F.T.C. 494 (2011).

[22] Scanscout, Inc., 152 F.T.C. 1019 (2011).

[23] Because Google's conduct allegedly constituted a violation of its 2011 FTC consent decree relating to its conduct in rolling out its Buzz social network, Google faced civil penalties for this infraction, and ultimately agreed to pay a record civil penalty of $22.5 million to settle charges related to its tracking of users on Safari. *See* United States v. Google, Inc., No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012).

[24] *See* Turn, FTC File No. 162-3024, https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter.

[25] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief, United States v. InMobi Pte Ltd., Case No.: 3:16-cv-3474 (N.D. Cal. filed June 22, 2016) [hereinafter InMobi Complaint], https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf.

[26] *See* 2012 Privacy Report, *supra* note 10, at 55.

[27] Epic Marketplace, Inc. & Epic Media Grp., LLC, 155 F.T.C. 406 (2013).

[28] *See* Sears Holdings Management Corp., FTC File No. 082-3099, https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter.

[29] FTC Administrative Complaint 2, Nomi Technologies, Inc. (Sept. 3, 2015) (emphasis added), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

[30] InMobi Complaint, *supra* note 25, ¶ 36.

[31] *Id.* ¶¶ 37–38.

[32] *See* Complaint Against Retro Dreamer for Permanent Injunction, Civil Penalties, and Other Relief, Case No.: 5:15-cv-2569 (C.D. Cal. filed Dec. 17, 2015), https://www.ftc.gov/system/files/documents/cases/151217retrodreamercmpt.pdf; Complaint Against LAI Systems, LLC for Permanent Injunction, Civil Penalties, and Other Relief, Case No.: 2:15-cv-9691 (C.D. Cal. filed Dec. 17, 2015), https:/www.ftc.gov/system/files/documents/cases/151217laicmpt.pdf?utm_source=govdelivery.

[33] *See* Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Speech, Am. Bar Ass'n 2017 Consumer Protection Conference 3, https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

[34] Steve Lohr, *Big Data Is Opening Doors, but Maybe Too Many*, N.Y. TIMES, Mar. 23, 2013, http://www.nytimes.com/2013/03/24/technology/big-data-and-a-renewed-debate-over-privacy.html.