

How Deep Packet Inspection Changed the Privacy Debate

*Ronald W. Del Sesto, Jr. and Jon Frankel**

September, 2008**

I. INTRODUCTION

Only recently have the legal perils of certain forms of online advertising come to light. Advertising in cyberspace provides enormous opportunities both to advertisers and the firms that provide the tools to support such advertising. For advertisers, online marketing holds the promise of narrowly focusing pitches to an audience most likely to be inclined to buy their products or subscribe to their services. For the companies developing the software to enable targeted marketing, the upside is enormous as more advertising dollars migrate to the web each year. One estimate indicates that spending for Internet advertising with a behavioral targeting component will soar from \$575 million last year to \$1 billion in 2008, and that still represents only 11 percent of the United States display, rich media, and video market.¹

A central component of online advertising is its unique ability to narrowly target marketing to specific groups of consumers. Since knowing the audience is a key factor to the success of these targeted advertisements, collecting as much information as possible about users is critical. Advertisers have used numerous tools over the past 10 years to collect this information and more recently, those tools are becoming more powerful and raising privacy concerns from consumer protection groups and policymakers.

Traditionally, online advertisers have engaged in “contextual advertising”—the practice of delivering ads based on the content of the webpage that the consumer currently is viewing or based upon a term that has been entered into a search engine. Recently, advertisers have begun using a sophisticated type of targeted marketing known as “behavioral advertising.” Behavioral advertising matches advertisements to a consumer’s interests based upon where that consumer surfs on the Internet over a period of time. For example, if a consumer visits various gardening websites, before viewing a travel site, the consumer could see a behaviorally-targeted garden advertisement displayed on the travel page, even though the travel page does not contain any gardening content. Many advertising networks that use behavioral targeting create consumer profiles by tracking users’ activities on publisher sites within their network. When the consumer visits a site where the ad network has purchased ad space, the ad network collects data about that visit while displaying an advertisement based on the consumer’s profile.²

* Ronald W. Del Sesto, Jr. and Jon Frankel are partners in the Telecommunications, Media and Technology Group at Bingham McCutchen, LLP, www.bingham.com.

** The references on page 10 to CDT, the Center for Democracy and Technology, have been corrected to refer to the Center for Digital Democracy.

1 *Behavioral Advertising on Target... to Explode Online*, June 11, 2007, www.emarketer.com.

2 *See generally, A Primer on Behavioral Advertising*, Center for Democracy and Technology Policy Post, July 31, 2008, available at <http://cdt.org/publications/policyposts/2008/12> (“*CDT Behavioral Advertising Primer*”)

The most recent development in online advertising technology is “deep packet inspection” or “DPI.” DPI permits advertisers to gain intimate knowledge of a users web browsing habits. DPI refers to the practice where an Internet Service Provider (“ISP”) installs certain equipment and software that allows it to monitor the web surfing habits of its customers. This information can be used to build valuable profiles about the online habits of each of the ISP’s customers. Accordingly, unlike the traditional models discussed above, with DPI technology, an advertiser partners with a consumer’s ISP, rather than a particular website or network of websites, to gather information potentially from all of a user’s searches and web data that only can be accessed by the ISP.³ That advertiser then serves targeted advertisements to users through an advertising network based upon the profile it has built from the information obtained from the ISP.⁴

The Federal Trade Commission (“FTC”) has been aware of the privacy issues associated with contextual and behavioral advertising for many years. Although Congress periodically has enacted laws addressing concerns relating to health information, children’s privacy, or industry-specific data practices—and while many states have enacted laws relating to the protection of personally identifiable information—the FTC historically has avoided broad ex ante proscriptions with respect to specific online advertising practices. The FTC has statutory authority with respect to privacy-related matters pursuant to several other federal statutes, including the Children’s Online Privacy Protection Act (regulating information concerning children), the Health Insurance Portability and Accountability Act (regulating health information), the Gramm-Leach-Bliley Act (financial information), the Telemarketing and Consumer Fraud Abuse Act (telemarketing), and the Fair Credit Reporting Act (consumer credit information). But instead of broad regulations, advertising in cyberspace has been governed by a loose assortment of consumer disclosures typically accomplished through privacy policies and user agreements. While website operators and application providers are exposed to potential legal liability for violating these agreements, enforcement generally is based on adherence to the agreements as drafted by the operator or service provider.

The FTC’s deliberate light regulatory touch may soon change as Congress increases its scrutiny of DPI in particular and the privacy concerns it raises. Both the House and Senate have held hearings and a variety of companies, including search engines, broadband providers, ISPs, and online advertisers, have received letters from legislators probing for detailed information about their online advertising practices. Certain legislators have questioned ISPs’ implementation of DPI and raised concerns about the legality of advertising based on the technology in the absence of affirmative consent from consumers.

³ *See Id.*

⁴ *See Deep Packet Inspection and Privacy*, Electronic Privacy Information Center, available at <http://epic.org/privacy/dpi/>.

This article will address some of the recent questions swirling around DPI. Specifically, we will examine why DPI has caused legislators to question the existing privacy regime. Also, we will analyze what the FTC has been doing prior to the advent of DPI and whether new privacy legislation will be enacted to address this advertising model. But first we will survey current events relating to online advertising in Congress.

II. CAPITOL HILL'S INTEREST IN BEHAVIORAL ADVERTISING

It is unclear what the catalyst was for Congress' sudden and intense interest in online advertising. Whatever the cause, in May, 2008, Rep. Edward Markey (D-MA) and Rep. Joe Barton (R-TX) sent a letter to a cable company upon learning about the company's plans to track websites visited by their customers and distribute this information to the advertising firm NebuAd. The letter questioned the company's practices. Following this inquiry, the recipient of the letter decided to delay its plans indefinitely. Similarly, on May 21, 2008, Rep. Barton sent a letter to Google asking questions related to its merger with Doubleclick.⁵

A. The Senate Examines Behavioral Advertising

On July 8, 2008, the Senate Committee on Commerce, Science and Transportation convened a full hearing regarding the privacy implications of online advertising. A number of different interests were represented at the hearing, however, notably absent were ISPs.⁶ The hearing generally served as an opportunity for the various participants to explain their positions with respect to online privacy and advise the Hill concerning the current state of the law and the underlying policies informing it.

Lydia Parnes, Director of the Bureau of Consumer Protection at the FTC, testified that the FTC believed that privacy concerns regarding online advertising can be addressed adequately by industry self-regulation that adheres to the FTC's proposed guidelines.⁷ According to Ms. Parnes, self-regulation is preferable for the dynamic marketplace because it affords the flexibility that is needed as business models continue to evolve.

Robert Dykes, Chairman and CEO of NebuAd⁸ at the time, testified that NebuAd does not collect or use personally-identifiable information ("PII")⁹ and provides users,

5 When the merger was announced by the companies in April, 2007, a number of parties quickly went on record opposing the merger for privacy reasons arguing that merging the data sets maintained by each company individually could be exploited in some manner disadvantageous to consumers and that federal regulators needed to address the risks associated with the online advertising by the combination.

6 Sen. Byron Dorgan (D-ND) stated that the ISPs had been invited to testify but declined, adding that he would call another hearing, focusing on the role of ISPs, and ask them to testify again. Ultimately, ISPs received letters from the House Committee on Energy and Commerce (see section C below).

7 The FTC's proposed behavioral advertising guidelines are discussed in Section IV below.

8 NebuAd is an online media company founded by Internet security experts in 2006. It provides online advertising in partnership with ISPs, using a select set of a user's Internet activities to construct anonymous inferences about the user's level of qualification with respect to a predefined set of market segment categories, which are then used to select and serve the most relevant advertisements to that user.

9 The FTC has defined "personally identifiable information" as any information that can be used to identify, contact, or locate a person, including information that may be linked with identifiable information from other sources, or from which other personally identifiable information can easily be derived. *Self-Regulation and Privacy Online: A Report to Congress*, July 1999 at FN 48 ("1999 Report"), available at <http://www.ftc.gov/os/1999/07/privacy99.pdf>.

and requires its ISP partners to provide users, with prior, robust, notice and the opportunity to choose whether to participate, both prior to service taking effect and during the service. Mr. Dykes also noted his belief of the common threads that run through privacy statutes throughout the United States and the European Community. Specifically, Mr. Dykes testified that disclosure and consumer consent is typically balanced against the type of information collected. More rigorous disclosure and consent typically is required under existing laws when more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer. Also, when raw data linked to an identifiable individual is stored for long periods of time, existing laws reflect an emerging trend that more stringent disclosure, consent, and security requirements should be imposed.

Mike Hintze, Associate General Counsel—Legal and Corporate Affairs of Microsoft Corporation, testified that online advertising is the main driver of the Internet economy and that online advertising continues to grow because it is interactive, targeted, relevant, and beneficial to advertisers because the targeted groups are more likely to buy the product. Mr. Hintze also noted that Microsoft supports the FTC’s efforts but advocates for a broader self-regulatory framework.

Leslie Harris, President and CEO of the Center for Democracy and Technology (“CDT”), a civil liberties group, testified in favor of stronger guidelines for behavioral advertising. Ms. Harris noted that while the practice of behavioral advertising is growing, consumers are increasingly uncomfortable with it and are unable to take meaningful steps to protect their privacy. According to Ms. Harris, even if told that behavioral advertising is necessary to continue the free Internet, consumers are still wary and uncomfortable with the practice.

Clyde Wayne Crews, Jr., the Vice President for Policy and Director of Technology Studies at the Competitive Enterprise Institute (“CEI”), testified regarding the advantages of a competitive market and voiced concerns regarding too much industry regulation, noting that user preferences and use preclude a one-size-fits all solution. According to CEI, “privacy dilemmas are inevitable on the frontiers of an evolving information era, but CEI maintains that competitive approaches to online privacy and security will be more nimble and effective than rigid political mandates at safeguarding and enhancing consumer well-being, facilitating commerce and wealth creation, and even contributing to the rise of the anonymous approaches to commerce we’d like to see.”

Jane Horvath, Google Incorporated’s Senior Privacy Counsel, testified about Google’s main advertising products and the benefits that Google believes online advertising brings to advertisers, online publishers, and individual Internet users. Ms. Horvath explained that Google makes privacy a priority because the success of its business model depends on it. If consumers do not feel their privacy is adequately protected by Google they are “only one click away” from switching to a competitor who offers more protection. Ms. Horvath also explained that Google looks to three design fundamentals as the bedrock of its business: (i) transparency; (ii) meaningful choice; and (iii) security. Finally, Ms. Horvath noted that Google supports comprehensive

federal privacy laws, supports the FTC's behavioral advertising principles (discussed in Section IV below) and believes greater labeling of online display advertising should be standard within the industry.

Chris Kelly, Chief Privacy Officer of Facebook Incorporated, testified about Facebook's privacy policies and procedures. Mr. Kelly said that all of their users have easy access to privacy settings and can control what information they share and who they share it with. He said that targeted advertising ultimately benefits users, but noted that Facebook never shares personal information with advertisers or other businesses.

B. The House Hearing on Behavioral Advertising and DPI

After the Senate hearings, the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet convened its own behavioral advertising hearing focusing specifically on DPI technologies. Members of the House Subcommittee and the witnesses all agreed that protecting users' privacy was important, but they disagreed on how to accomplish that goal. Generally, the legislators insisted that consumers should have to actively agree to have their online surfing information tracked by ISPs. In other words, some House members believed that the only legitimate and, in some cases, legal way to engage in DPI and behavioral advertising practices would be to have consumers provide affirmative consent where they either click or check a box that expressly informs them of what type of information is being collected about them and how it will be used. This type of consent is referred to as "opt-in." But, as most of the witnesses testified, this view is at odds with how consumers currently are provided with a choice whether the information collected about their online activities can be used for marketing purposes. That is, traditionally most companies provide their customers with notice through a privacy policy or other agreements that allow the company to use personal information unless the user specifically does not consent to such use. This is referred to as "opt-out" consent.¹⁰

In his opening remarks, Subcommittee Chairman Edward Markey stressed that privacy is a cornerstone of freedom and that he would support legislation to protect consumers' privacy where needed. He urged broadband providers to adopt clear privacy policies related to DPI that should include at a minimum: (1) a clear and conspicuous public notice of how consumer information will be used by the provider; (2) an affirmative opt-in provision; and (3) if a consumer opts-out, the broadband provider should immediately cease monitoring that consumer's actions on the Internet.

Rep. Cliff Stearns suggested that the scope of the hearing be expanded beyond the focus on network providers and to include online search engines. He cautioned however, that DPI legislation may be premature at this juncture and that any new legislation could end up inadvertently harming small businesses who need targeted advertising to compete with larger companies.

¹⁰ The fact that the opt-in versus opt-out debate became so contentious during these hearings is not surprising. The debate over how consumers consent to the sharing of their personal information has been one of the most controversial issues in Internet privacy over the last five years and continues to be the key issue with respect to online privacy generally.

Testimony was provided by a number of different interests,¹¹ although once again ISPs were not present at this hearing. Dr. Reed from MIT provided highly technical testimony concerning how DPI works and indicated that DPI technologies are particularly worrisome because they involve inspection of end-user to end-user information content, decoding, and the making of inferences about users' personal interests, private activities, health information, and other personal details that many people would likely not willingly allow access to for advertising purposes.

Scott Cleland, President of Precursor LLC, an industry research and consulting firm and Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies, stressed that the current patchwork of U.S. privacy laws, the lack of a holistic approach to Internet privacy, and selective oversight of privacy problems have combined to create perverse incentives for some companies to arbitrage privacy laws and push the privacy envelope.

Bihan Sabet from Spark Capital, a venture capital firm that makes investments in early stage companies in the Internet, media and technology industries, testified that there is nothing wrong with DPI as it can provide significant economic and consumer benefit if used correctly. He cautioned that lawmakers need to understand the impact of DPI and how legislation could impact the open Internet and the Internet ecosystem. According to Mr. Sabet, leaving the Internet free from unnecessary regulation encourages investment and innovation.

Ranking Member Cliff Stearns noted that both search engines and broadband providers use tailored Internet advertising standards and identified "the core question" as whether clear opt-out standards are sufficient or should be replaced by explicit opt-in requirements. Other members of the Subcommittee, including Rep. Gene Green, Rep. Bart Stupak, and Rep. Greg Walden expressed the concern that explicit opt-in consent was needed prior to data collection or tracking, and Rep. Mike Doyle noted that "no one" reads the opt-out notices in privacy statements or other bill inserts and that consumers do not know that silence constitutes implied consent.

C. Letters to ISPs, Search Engines and Broadband Providers from the House Committee on Energy and Commerce

Following the House hearings, the Subcommittee sent letters to 34 companies inquiring about their online advertising activities and privacy practices. Some of the information sought by the Subcommittee included whether the recipient had engaged in tailored advertising and, if so, in what communities, the nature of the information

¹¹ The following individuals testified at this hearing: (i) Mr. Dykes; (ii) Bihan Sabet, General Partner, Spark Capital; (iii) Alissa Cooper, Chief Computer Scientist, Center for Democracy and Technology; (iv) Dr. David P. Reed, Adjunct Professor, the Media Lab, Massachusetts Institutes of Technology; and (v) Scott Cleland, Precursor, LLC; Chairman, Netcompetition.org. NebuAd and CDT's testimony was similar to what they said during the Senate Hearing, although CDT did urge the Subcommittee to seek additional information directly from ISPs and their partners about how they are using DPI.

collected, the data retention practices adopted by recipients that engaged in such practices, whether the recipient obtained opt-in or opt-out consent, a copy of the text of the notice that the recipient provided to users, and whether the recipient analyzed the legal issues associated with engaging in such practices. Letters were sent to ISPs, including cable and telephone companies, and online search engines. The responses were made public demonstrating that six of the recipients had either trialed or implemented DPI. Typically, these companies updated their privacy policies or terms of use in order to obtain consumer consent to the practice, i.e., they followed an opt-out regime. But 24 of the recipients either did not track their consumers online activity at all or did so only among the websites they owned or controlled. Three recipients disclosed that they track their users among various websites, not just ones they own or control, but do not engage in DPI. The balance indicated that they have considered various forms of online advertising but do not currently engage in any form of online tracking.

Subsequent to the Hill hearings and letters, many of those companies either engaging in or considering DPI have since abandoned it. Further, NebuAd is suspending sales of its product that users DPI and has asked ISPs to suspend use of the product. It would appear that any current concerns relating to DPI will not merit another House hearing prior to the election given the fact that the practice has been abandoned by all of the companies that publicly acknowledged to using DPI. But Rep. Markey has indicated that he would like to further investigate DPI, online advertising and what would constitute an effective comprehensive privacy regime.

III. CHALLENGES TO LEGALITY OF BEHAVIORAL ADVERTISING

As the behavioral advertising debate has pushed itself into the public consciousness, several participants have increased the pressure on legislators and regulators to take action by arguing that behavioral advertising partnerships between ISPs and advertisers may violate federal and state laws. Specifically, on the eve of the Senate hearings,¹² CDT released a report suggesting that ISPs selling or otherwise providing their subscriber activity to online advertisers may violate state and federal surveillance laws.¹³

The *CDT Wiretap Report* argues that the federal Wiretap Act, as amended by the Electronic Communications Privacy Act (“ECPA”), prohibits the interception and disclosure of electronic communications—including Internet traffic content—without

¹² See *supra* Section II.a.

¹³ See *An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising*, Center for Democracy and Technology, July 8, 2008 (<http://www.cdt.org/privacy/20080708ISPtraffic.pdf>) (the “CDT Wiretap Report”). Similarly, on May 16, 2008 at a Digital Frontiers Conference at Stanford University, Lee Tien, a senior research attorney at the Electronic Frontier Foundation argued that companies that create and use programs to intercept communications between users and the Web sites they visit in order to send targeted advertising likely violate the federal Wiretap Act and other federal laws.

consent.¹⁴ And, that although the ECPA has exceptions to this rule that permit interception and disclosure without consent, CDT argues that those exceptions do not apply to the interception or disclosure of Internet traffic content for behavioral advertising purposes. The *CDT Wiretap Report* then concludes that the ECPA requires unavoidable notice and affirmative *opt-in* consent before Internet traffic content may be used from ISPs for behavioral advertising purposes.”¹⁵

While there is little question that the *CDT Wiretap Report* has added fuel to the growing behavioral advertising fire, there does not appear to be any case law that directly applies the ECPA to preference marketing. Thus, while behavioral advertising arguably includes a certain degree of surveillance and likely is an electronic communication under the ECPA, existing case law does not explicitly address the application of the ECPA to tracking users’ online activities.

In addition to CDT’s arguments concerning the application of the ECPA, several members of Congress have noted that the Cable Communication Policy Act (“CCPA”) also may apply to behavioral advertising.¹⁶ Specifically, certain House members have argued broadly that any service that collects information about the web-related habits and interests of a subscriber without first obtaining written or electronic consent to such collection raises “substantial questions” under the CCPA.¹⁷

IV. REGULATION AND SELF REGULATION —THE FTC’S APPROACH TO BEHAVIORAL ADVERTISING

Although behavioral advertising has been a hot button topic in Congress in recent months, the debate over whether and how to regulate the practice of gathering information about consumers’ online activities has been going on for over ten years. A summary of this decade-long debate is instructive as to how the behavioral advertising quandary ultimately may be resolved, particularly since the FTC likely will be involved in its resolution.

In 1998, the FTC released a report that identified “notice, choice, access, and security” as key elements of online fair information practice principles.¹⁸ This *1998 Report* also identified “enforcement” as a critical component of any governmental or self-regulatory program to protect privacy online, but stopped short of proscribing any specific requirements for privacy policies and practices. The FTC noted that it had for several years “encouraged industry to address consumer concerns regarding online privacy through self-regulation” on the basis that effective self-regulation would

¹⁴ 18 U.S.C. § 2511.

¹⁵ The CDT Wiretap Report also suggests that ISP advertising partnerships violate state laws requiring all-party consent to interception.

¹⁶ House Representative Edward Markey and House Representative Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008) http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf (the “Charter Letter”).

¹⁷ See *Charter Letter* at 1. Ultimately, Charter decided not to partner with NebuAd for its services.

¹⁸ *Privacy Online: A Report to Congress*, June 1998 (“1998 Report”), available at <http://www.ftc.gov/reports/privacy3/toc.shtm>.

better permit “firms to respond quickly to technological changes and employ new technologies to protect consumer privacy.”¹⁹ The FTC found, however, that this self-regulatory approach had failed to yield practices consistent with the principles it had articulated, and that enforcement mechanisms were particularly lacking.²⁰

Despite these findings, in 1999, the FTC continued to recommend to Congress that self-regulation be given more time to prove effective, and thus, called upon the industry to make greater efforts in implementing the fair information practice principles set forth in the *1998 Report*.²¹ In response to this request and “consumer concerns over the use of profile-based targeted online advertising,” the Network Advertising Initiative (the “NAI”) was formed in 1999.²² The NAI is an industry group comprised of some of the largest participants in the network advertising industry, representing over 90% of the industry in terms of revenues and ads served earlier this decade.²³ Within a year of its formation, the NAI adopted a set of self-regulatory principles (the “*NAI Principles*”) with respect to “online preference marketing,” based in part upon input from the FTC and the Department of Commerce.²⁴

In the wake of the release of the *NAI Principles*, the FTC released a series of reports to Congress relating to online profiling and privacy, addressing many of the same issues that are now captured in the phrase “behavioral advertising.”²⁵ First, in May 2000, the FTC released an update to the *1998 Report*, detailing “continued improvement” in website privacy disclosures and the nascent development of “online privacy seal programs” that would measure companies’ efforts to implement fair information practices.²⁶ The FTC, however, noted that industry compliance with such principles was not yet widespread enough for its liking. Moreover, although it noted that “there will continue to be a major role for industry self-regulation in the future,” the FTC recommended for the first time that Congress enact legislation to require implementation of the standards identified in the *1998 Report*.²⁷ In a separate report to Congress specifically addressing “online profiling” issued shortly thereafter, the FTC reiterated that industry proposals such as the *NAI Principles* were laudable, but that “backstop legislation” addressing online profiling would be required “to fully ensure that consumers’ privacy is protected online.”²⁸ Yet, at the same time, the FTC effectively endorsed the *NAI Principles* and seemingly endorsed the self-regulatory approach they represented.²⁹

¹⁹ *Id.* at Section VI.

²⁰ *Id.*

²¹ *1999 Report* at 12.

²² *About Us*, NAI website, available at <http://networkadvertising.org/about/>.

²³ *Online Profiling: A Report to Congress*, Part 1, June 2000 (“2000 Report Part 1”), available at <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>; and Part 2, July 2000 (“2000 Report Part 2”), available at <http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>, citing to 2000 Report Part 2 at 10.

²⁴ The full text of the *NAI Principles* is available at http://www.networkadvertising.org/pdfs/NAI_principles.pdf.

²⁵ See *2000 Report Part I* and *2000 Report Part II*.

²⁶ “*Privacy Online: Fair Information Practices in the Electronic Marketplace - A Report to Congress*,” May 2000, at ii, available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

²⁷ *Id.* at iii.

²⁸ *2000 Report Part II* at 10.

²⁹ *Id.*; see also “*FTC Endorses Privacy Principles*,” *Wired Magazine*, July 27, 2000, available at <http://www.wired.com/politics/law/news/2000/07/37853>.

Despite all this activity concerning online privacy between 1998 and 2000, there surprisingly was little legal, regulatory or political activity in this area until 2006 when the FTC held its “Tech-ade” event and behavioral advertising generated substantial debate.³⁰ One can speculate as to a variety of economic, structural, technological, regulatory, and/or political reasons why potential regulation of targeted advertising generated such substantial debate in 1999 and 2000 but then failed to attract any significant attention from the FTC until it again became a focus during the 2006 “Tech-ade” hearings. Regardless of the reasons for this gap in time, however, the “Tech-ade” event resurrected the behavioral advertising debate.

And arising out the Tech-ade hearings, the FTC staff “held many dozens of meetings with consumer representatives, industry members, academics, technologists, and others to gain a better understanding of current and anticipated online advertising models.”³¹ The FTC then scheduled a “Town Hall” in November 2007 to address specifically how behavioral advertising had changed in recent years and discuss the effectiveness of regulatory and self-regulatory measures aimed at consumer protection.

In addition, in the wake of the Town Hall meeting and in an apparent effort to reignite action with respect to behavioral advertising, the Center for Digital Democracy and the US Public Interest Research Group filed a Supplemental Statement in support of their *November 2006 Complaint* regarding allegedly unfair and deceptive online marketing practices. In the supplemental statement, these organizations renewed their request for an investigation into data collection and behavioral advertising practices, and linked the perils of such activities to issues as wide-ranging as social networking, racial profiling, and the sub-prime mortgage crisis.³²

³⁰ See *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, FTC Staff Statement, Dec. 20, 2007 (“*Staff Statement*”) at 1, <http://www.ftc.gov/os/2007/12/P85990ostmt.pdf>. See also *Privacy Self Regulation: A Decade of Disappointment*” Electronic Privacy Information Center, March 4, 2005, at 5 (“*EPIC 2005 Report*”). (“The overall effect of the FTC’s approach has been to delay the adoption of substantive legal protection for privacy. The adherence to self-regulatory approaches, such as the [NAI Principles] that legitimized third-party Internet tracking ..., allowed businesses to continue using personal information while not providing any meaningful privacy protection.”) On November 1, 2006, at around the same time as the Tech-ade event, the Center for Digital Democracy and the US Public Interest Research Group filed a *Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices* (“*November 2006 Complaint*”). The *November 2006 Complaint* requested that the FTC recommend Congressional action requiring affirmative consent with respect to all use of consumer data (without clear distinction as to PII or non-PII data).

³¹ *Staff Statement* at 1.

³² See Center for Digital Democracy and the US Public Interest Research Group Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices, at 72-73 (“*Supplemental Statement*”). Other events in 2007 also likely contributed to the increased interest in behavioral advertising. First, the uproar over Facebook’s Beacon feature—which reports on users’ visits to third-party websites—drew significant press attention in late 2007. See, e.g., *Facebook apologizes, pulls back on social ads*, SFGate.com, Dec. 6, 2007. Second, in April 2007, Google announced that it would acquire DoubleClick. The acquisition was opposed by a number of parties on the grounds that the combination of their consumer information data sets could be exploited in some manner and that the FTC needed to address risks associated with behavioral advertising by the companies. See Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170. at 2. The FTC closed its investigation of the acquisition in December 2007.

As a result of the Town Hall meeting, and perhaps the *Supplemental Statement* too, the FTC issued its *Staff Statement* on behavioral advertising. The *Staff Statement* attempts to adopt a neutral position in posing questions about “behavioral advertising” and specifically positions itself as *considering* “self-regulatory” principles. Most importantly, the *Staff Statement* is not a rule or regulation but rather just “proposed principles to guide the development of self-regulation in this evolving area.”³³ As an initial matter, the *Staff Statement* adopts a broad definition of online “behavioral advertising.” In the FTC’s view, similar to its prior definition of “online profiling,” “behavioral advertising” means “the tracking of a consumer’s activities online, 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.”³⁴ The FTC staff has promulgated the following proposed principles “to encourage more meaningful and enforceable self-regulation to address the privacy concerns raised with respect to behavioral advertising:”³⁵

- **Transparency and Consumer Control.** The FTC has proposed that every website where data is collected for behavioral advertising provide a “clear, concise, consumer-friendly and prominent statement” that (a) “data about consumers’ activities is being collected at the site for use in providing advertising about products and services tailored to individual consumers’ interests;” and (b) “consumers can choose whether or not to have their information collected for such purpose.” The website also should provide an easy-to-use method for exercising this option.
- **Security and Data Retention.** The FTC has proposed that any company that collects and/or stores consumer data for behavioral advertising provide “reasonable security” for that data, based upon the sensitivity of the data, the nature of a company’s business operations, the types of risks a company faces, and the reasonable protections available. In addition, a company should retain data “only as long as is necessary to fulfill a legitimate business or law enforcement need.”
- **Affirmative Express Consent for Privacy Policy Changes.** The FTC previously has determined in one case that “opt in” consent should be required if material changes made to a privacy policy would affect data collected under a prior version of the policy. The FTC apparently proposes to codify and/or reaffirm that approach through the proposed principles here.
- **Affirmative Express Consent for Use of Sensitive Data.** The FTC has proposed that companies only collect sensitive data (e.g., health information, children’s activities online, etc.) for behavioral advertising after obtaining “opt in” consent from the consumer that such data can be used in connection with such advertising. The FTC seeks comment as to what types of information should be defined as “sensitive,” and whether certain data may be too “sensitive” for use in behavioral advertising even with express consumer consent.

33 See *FTC Staff Proposes Online Behavioral Advertising Privacy Principles*, Press Release, December 20, 2007, <http://www.ftc.gov/opa/2007/12/principles.shtm>.

34 *Staff Statement* at 2.

35 *Id.* at 3.

- **Use of Tracking Data for Purposes *Other than Behavioral Advertising*.** The FTC seeks information about how tracking data might be used for purposes other than behavior advertising. In particular, the FTC has asked what secondary uses might exist, what concerns they raise, and whether some heightened level of protection is required.

The FTC proposals are open-ended in nature, leaving advertisers, web publishers, ISPs and other interested parties to fill in a rather blank canvas. Moreover, it remains unclear at this point the degree to which the FTC's supposed "self-regulatory" principles are truly intended as guidance for self-regulation, or whether they will be used as an underpinning for substantive regulation. It also is noteworthy that the NAI recently announced an intent to revisit its own principles in what would seem to be an effort to forestall further legislative or regulatory action much as it did through adoption of the original *NAI Principles* in 2000.³⁶ Thus, the remainder of 2008 and 2009 appear poised to be an active and important period in defining how companies will be able to engage in the collection, use, retention, and sharing of consumer data online for marketing purposes going forward.

CONCLUSION

While a myriad of factors led to recent public scrutiny of advertising in cyberspace, it would appear that the use of sophisticated software tools allowing for the development of detailed online profiles made possible by DPI, coupled with the FTC's light regulatory touch, largely created the current political climate. Prior to DPI, privacy concerns could be addressed by users blocking websites from tracking their movement through their web browsers and other tools.³⁷ Similarly, privacy is not as big a concern where advertisers use contextual based advertising based on user generated search terms. The advent of DPI, however, changed the online advertising landscape and raised serious concerns as to whether consumers were provided with a meaningful opportunity to consent to the use of technology that allowed for the collection of all sorts of information relating to consumers habits in cyberspace. Thus, while opt-out consent did not cause any public alarm when associated with traditional forms of online advertising, DPI changed everything.

Armed with arguments that DPI could collect significant amounts of personal information, including potentially sensitive personal information, privacy advocates argued to legislators that consumer must provide affirmative opt-in consent before ISPs and advertisers could use this powerful new technology. Moreover, privacy advocates argued that the FTC's self-regulatory regime was enacted before anyone

³⁶ "NAI Announces 2008 Behavioral Advertising Principles Initiative," Press Release, Jan. 3, 2008, available at <http://www.networkadvertising.org/networks/bto10308.asp>.

³⁷ For instance, users can opt-out of all targeted advertising by NAI members simply by visiting the NAI website (see www.networkadvertising.org/optout_nonpii.asp). Also, consumers generally can disable cookies on their computer to prevent certain tracking of their online activities.

truly understood the capabilities of DPI. As a result, privacy advocates were able to argue that new technologies had changed the online marketing reality for consumers so drastically that the industry was in need of reform or that new legislation was required to protect consumers. It is unclear whether this issue will have enough political momentum to result in legislation by the new Congress. For now DPI remains a controversial practice that is sure to keep a variety of players in the online privacy debate engaged for years to come.

Boston
Hartford
Hong Kong
London
Los Angeles
New York
Orange County
San Francisco
Santa Monica
Silicon Valley
Tokyo
Walnut Creek
Washington

bingham.com

© 2008 Bingham McCutchen LLP

One Federal Street, Boston, MA 02110

ATTORNEY ADVERTISING

To communicate with us regarding protection of your personal information or if you would like to subscribe or unsubscribe to some or all of Bingham McCutchen LLP's electronic and mail communications, please notify our privacy administrator at privacyUS@bingham.com or privacyUK@bingham.com. Our privacy policy is available at www.bingham.com/privacy.asp. We can also be reached by mail in the U.S. at One Federal Street, Boston, MA 02110-1726, ATT: Privacy Administrator, or in the U.K. at 41 Lothbury, London, England EC2R 7HF, ATT: Privacy Administrator, or by telephone at 866.749.3064 (U.S.) or +08 (08) 234.4626 (International).

Bingham McCutchen (London) LLP, a Massachusetts limited liability partnership regulated by the Solicitors Regulation Authority, is the legal entity which operates in the UK as Bingham. A list of the names of its partners and their qualifications is open for inspection at the address above. All partners of Bingham McCutchen (London) LLP are either solicitors or registered foreign lawyers.

This communication is being circulated to Bingham McCutchen LLP's clients and friends. It is not intended to provide legal advice addressed to a particular situation. Prior results do not guarantee a similar outcome.