Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience

Andrea N. Person*

* Andrea N. Person graduated from the American University School of International Service in 2005 and holds a Bachelor of Arts degree in international studies with a concentration in international communications. She expects to complete her Juris Doctorate degree from the Indiana University Maurer School of Law in May 2010. Andrea would like to thank Amy Andryszak, Jill Cocayne, and David Hoover for helping her stay on top of the behavioral advertising debate from outside the Beltway. She would also like to thank the FCLJ editorial staff and Senior Board for their help in editing this Note.

I. INTRODUCTION

Like antibiotics, cars, and the microwave, the Internet has revolutionized the way people live. Over the last decade, the online community has become a day-to-day utility for the average person who, on any normal day, sends e-mails, makes calls, orders groceries, makes reservations, catches up on the news, and goes shopping. However, as technology becomes more advanced, the risks associated with it also increase. Laws must be carefully drafted to allow the continued development of technology while insuring that people are protected online. Policymakers who are fearful of the consequences of having personal information available online have made protecting that information a top priority. In their quest to limit information breaches online, government officials have recently focused on behavioral advertisements as the issue du jour. Behavioral advertising is a broad concept on the Internet, though, and defining what the government means by regulation in this space is complicated.

Deep packet inspection technology (DPI) is one technology platform that is being used to provide behavioral advertising to online customers. Some policymakers believe that this technology should be regulated because they are fearful that the technology grants companies too much access to personal information online. In particular, these policymakers have raised concerns with the use of this information for creating behavioral advertising profiles.[1] Responding to the lack of U.S. law dealing

1. *See* 154 CONG. REC. D915 (daily ed. July 17, 2008) (notice of Committee Meeting, *H. Comm. on Energy and Commerce, Subcomm. on Telecomm. and the Internet* hearing entitled *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies*); 154 CONG. REC. D1174 (daily ed. Sept. 25, 2008) (notice of Committee Meeting, *S. Comm. on Commerce, Science, and Transportation* hearing entitled *Broadband Providers and Consumer Privacy*); 155 CONG. REC. D1333 (daily ed. Nov. 16, 2009) (notice of Committee Meeting, *H. Comm. on Energy*

with behavioral advertising, congressional leaders in the 110th and the 111th Congresses held hearings in both houses to learn about the technology and the regulatory issues that surround it.[2] The first hearings began during the summer of 2008. No direct legislation came of those hearings, but the sentiment of policymakers signaled a commitment to focus on this hot-button issue. The commitment was honored as more hearings on the issue took place throughout 2009.[3] Despite the fact that, at the time of publishing, no legislation had been filed, the chairman of the House Subcommittee on Communications, Technology, and the Internet, Rick Boucher, continues to list privacy legislation that focuses on this issue as one of his top priorities.[4] While protecting the personal information of Americans online should be a top priority, it is equally important to consider how regulation in this area may affect the future of the Internet and how too much regulation may harm the consumer.

This Note asks how increasing regulatory barriers to limit online behavioral advertising could affect the consumer's experience online. To answer this question, this Note first looks at what DPI is, who uses it, and its purposes. Second, this Note discusses U.S. court decisions and policy decisions, as well as international business trials that relate to DPI and behavioral advertising practices. Specifically, this Note looks at the actions of the Federal Trade Commission (FTC) and Congress in responding to DPI. Finally, this Note proposes reforms for policymakers to consider as they continue to contemplate regulations for DPI.

The Internet is a terrific power for increasing wealth, knowledge, and communication. As the Internet continues to grow in day-to-day importance, regulations must be carefully drafted to ensure that online experiences are enhanced and not limited. Congress should not set a precedent by shutting the door to DPI because the technology seems to present privacy problems; instead, policymakers should recognize that there are benefits to the technology and create a light-touch regulatory environment where the technology—and others like it—can thrive and consumers can benefit.

---

and Commerce, Subcomm. on Commerce, Trade and Consumer Protection and *Subcomm., on Comm., Tech., and the Internet*, joint hearing entitled *Exploring the Offline and Online Collection and Use of Consumer Information*); *see also* 155 CONG. REC. D432 (daily ed. April 22, 2009) (notice of Committee Meeting, *H. Comm. on Energy and Commerce, Subcomm. on Comm., Tech., and the Internet*, hearing entitled *Communications Networks and Consumer Privacy: Recent Development*).

2. *See supra* note 1.

3. *See* 155 CONG. REC. D1333, *supra* note 1; *see also* 155 CONG. REC. D432, *supra* note 1.

4. Rick Boucher, *Boucher: Expanding Access Remains the Goal*, ROLL CALL, Dec. 14, 2009, http://www.rollcall.com/features/Agenda-Ahead_2009/agenda_ahead/41410-1.html.

II. DEEP PACKET INSPECTION TECHNOLOGY

Deep Packet Inspection technology provides Internet service providers (ISPs) with the ability to collect all Internet communications made by a consumer.[5] Depending on how the technology is deployed, it may "monitor[], analyze[], and potentially manipulate[] Internet traffic."[6] DPI accomplishes these actions by "taking a magnifying glass to the individual packets of data that traverse the network."[7]

A. How Deep Packet Inspection Technology Works

When DPI technology is deployed, it first collects the information that consumers view online. To do this, DPI collects packets. On the Internet, packets combine to create online communications such as "Web browsing, e[-]mail, [V]oice-over-I[nternet] P[rotocol] (VoIP) phone calls, peer-to-peer ([P2P]) file transfers, [and] online gaming," among others.[8] Frequently, packets are analogized to an envelope containing a letter.[9] Like a letter, the packet includes a message or "a 'payload,' which is the actual data inside the packet . . . and a 'header,'" which is similar to an envelope that can direct the packets to the correct recipient.[10] Normally, routers throughout the system read the header information and, like a post office, determine where the information should be sent—a process called "shallow packet inspection."[11] Shallow packet inspection does not look at the contents of the packet; instead, it acts as a mechanism to move the packets where they need to go. Because shallow packet inspection is only a routing mechanism, it does not expose personally identifiable information (PII) embedded in a message, and communications are virtually anonymous.[12]

---

5. KATHLEEN ANN RUANE, CRS REPORT FOR CONGRESS, PRIVACY LAW AND ONLINE ADVERTISING: LEGAL ANALYSIS OF DATA GATHERING BY ONLINE ADVERTISERS SUCH AS DOUBLECLICK AND NEBUAD (2008); Memorandum from the *U.S. House of Representatives Comm. on Energy and Commerce* staff to the *Subcomm. on Telecomm. and the Internet* members and staff regarding the hearing on *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Comm. Laws and Policies* (July 16, 2008) (on file with author) [hereinafter Memorandum].

6. Memorandum, *supra* note 5, at 1.

7. *Id.* at 2.

8. *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong., at 5 (2008) (statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology), *available at* http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Cooper-testimony.pdf [hereinafter Statement of Alissa Cooper].

9. *Id.* at 4-5.

10. *Id.*

11. *Id.* at 5; Memorandum, *supra* note 5, at 2.

12. Statement of Alissa Cooper, *supra* note 8, at 5; *see also* Memorandum, *supra* note

DPI, however, looks past the "header" to the "payload," where detailed information regarding the message that the consumer is trying to send is located.[13] Depending on the technology, the payload information that it reads varies. Narus DPI technology, for example, claims to have the capability to "look inside all traffic from a specific IP address, pick out the HTTP traffic, then drill even further down to capture only traffic headed to and from Gmail, and can even reassemble e-mails as they are typed out by the user."[14] However, application analysis or "network intelligence" is a less intrusive and more basic use of DPI.[15] This type of analysis looks at the application or protocol signature to see what type of application is being used.[16] Network intelligence analysis provides detailed accounts of the number of consumers surfing the Web, downloading content, utilizing VoIP, participating in P2P technology, or even distributing a virus at any given time.[17] Currently, DPI provides information about the online tendencies of Internet users, by reviewing search engine queries, recognizing trends with the frequency of consumer Web site visits, and recording the types of applications that consumers are using online.[18]

B. The Many Pieces of the DPI Puzzle

The original motivation for DPI technology was to prevent online security breaches.[19] Primarily, the technology was invented to minimize the harmful effects of Internet viruses by intercepting malicious programs before they reached end users.[20] Private and commercial networks used DPI's ability to read packets at the application level to offer high-level protection by monitoring the transmission of programs. In addition to ensuring personal security, DPI has been used by law enforcement to conduct surveillance over ISPs and to comply with the Communications Assistance for Law Enforcement Act (CALEA) requirements.[21] Recently,

---

5, at 2. Debate exists over if PII should include the individual user's IP address that is used when accessing the Internet. Kenneth Corbin, *FCC Looks Ahead to Net Neutrality: Privacy Top Agency Advisors Look Ahead to the Simmering Issues Likely To Boil over this Year at the FCC*, INTERNETNEWS.COM, Apr. 6, 2009, http://www.internetnews.com/government/article.php/3813751/FCC+Looks+Ahead+to+Net+Neutrality+Privacy.htm.

13. Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, ARS TECHNICA, July 26, 2007, http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars/.

14. *Id.*

15. Memorandum, *supra* note 5, at 2.

16. *Id.*

17. *Id.* at 2-4.

18. *Id*. at 2-5.

19. *Id.* at 4.

20. *See id.*

21. *Id.*

the technology has worked to stop copyright infringement violations. In January 2008, AT&T announced that it would notify the copyright holder if it detected an infringement occurring on its network.[22] At that time, AT&T further stated that the company would go as far as to block service to customers if it detected that those customers were transmitting "illegally obtained copyrighted works" over its network.[23]

DPI has also been used to manage networks and tier service offerings. The technology became the focus of an FCC Order in 2008 when Comcast used it to recognize P2P file sharing on its network and degrade service to customers who were participating in those types of communications.[24] The FCC reacted to Comcast by forcing it to discontinue use of those management techniques.[25] Comcast appealed the FCC decision in September 2008 on the grounds that the FCC lacked authority to regulate in that area.[26] On April 6, 2010, the D.C. Circuit vacated the FCC decision in favor of Comcast holding that the FCC does not have jurisdiction in this area.[27]

Like Comcast in the United States, broadband service providers abroad use DPI to manage networks and tier services. Tiering allows ISPs to sell heavy users more bandwidth capacity while allowing smaller bandwidth users to save money by purchasing less capacity.[28] Already, this practice is common in the United Kingdom where services like PlusNet sell broadband accessibility by the gigabyte and pair routers with varying

---

22. *Id.*

23. *Id.* at 5. *See also* James S. Granelli, *AT&T To Target Pirated Content*, LA TIMES, June 13, 2007, *available at* 2007 WLNR 11002484.

> Last week, about 20 technology executives from Viacom Inc., its Paramount movie studio and other Hollywood companies met at AT&T headquarters to start devising a technology that would stem piracy but not violate privacy laws or Internet freedoms espoused by the Federal Communications Commission.
>
> Cicconi said that once a technology was chosen, the company would look at privacy and other legal issues.
>
> "We are pleased that AT&T has decided to take such a strong, proactive position in protecting copyrights," Viacom said in a prepared statement. "AT&T's support of strong anti-piracy efforts will be instrumental in developing a growing and vibrant digital marketplace and will help ensure that they have a steady stream of great creative content to deliver to their consumers."

Id.

24. Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, *Memorandum Opinion and Order,* 23 F.C.C.R. 13028 (2008).

25. *Id.* at para. 54.

26. *See* Yinka Adegoke, *Comcast Files Appeal of FCC Web Traffic Order,* REUTERS, Sept. 4, 2008, *available at* http://www.reuters.com/article/internetNews/id USN0442726520080904.

27. Comcast Corp. v. FCC, No. 08-1291 (D.C. Cir., Apr. 6, 2010), *available at* http://pacer.cadc.uscourts.gov/common/opinions/201004/08-1291-1238302.pdf.

28. Anderson, *supra* note 13.

degrees of capacity to the type of bandwidth the user purchases.[29]

C. The Issue du Jour—Behavioral Advertising

Behavioral advertising has recently risen in the public spotlight as another major way that DPI technology is used. Behavioral advertising caters to the specific desires and preferences of a particular consumer.[30] In order to advertise in this manner, corporations must gather large quantities of information detailing a consumer's preferences. DPI technology then analyzes the Web traffic of consumers and compiles a "record of Web use (largely based on the existence of specific words in a packet) to develop an advertising profile for a particular customer or group of customers."[31] This results in individualized advertisements that follow the consumer across the Internet and directly pertain to his or her demonstrated interests.[32] In testimony before the U.S. Senate Committee on Commerce and Technology in 2008, former NebuAd CEO Bob Dykes said that Internet advertising using DPI "permits advertisers to provide more relevant messages to consumers and in turn fuels the development of [Web site] publishers both large and small."[33] Former U.S. market leader, NebuAd, found itself at the center of the behavioral advertising debate in the United States in 2008 due to congressional concern over its partnerships with ISPs and, as a result, went out of business.[34] According to testimony before the House during the summer of 2009, witnesses signaled that no company in the United States presently was providing the service.[35]

D. Cookies and Deep Packet Inspection Technology—A Progression of Technologies

Behavioral advertising is not new. Traditionally, behavioral advertisement profiles were compiled through the use of Web site–based

---

29. *Id. See also* PlusNet, http://www.plus.net/ (last visited Apr. 7, 2010).

30. Memorandum, *supra* note 5, at 3; FTC, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf (defining behavioral advertising as "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").

31. Memorandum, *supra* note 5, at 3.

32. *Id*.

33. *Privacy Implications of Online Advertising Before the S. Comm. on Commerce, Science & Transportation*, 110th Cong. (2008) (statement of Bob Dykes, CEO, NebuAd) [hereinafter Statement of Bob Dykes].

34. Deborah Yao, *NebuAd Closing Doors After Internet Policy Woes*, USA TODAY, May 21, 2009, *available at* http://www.usatoday.com/tech/techinvestor/corporatenews/2009-05-21-nebuad_N.htm.

35. Statement of Bob Dykes, *supra* note 33.

"cookies."[36] While DPI provides a stream of information about an individual across Internet portals, cookies provide information from data files that are placed on an Internet user's computer hard drive when that user visits an affiliated Web site.[37] Once in place, Web site operators and their agents can use cookies to obtain information about users. Information gathered by cookies can include passwords that are connected to the site or preferences that the user may have while online.[38] Cookies can be malicious or beneficial to the online experience. Malicious cookies may appear as spyware and work to install viruses or slow down a computer's operating system.[39] The static nature of cookie technology makes it very different than the dynamic nature of DPI technology because cookies are only able to access a predetermined amount of information.[40] The fear associated with DPI is that it is capable of accessing the complete communications of a user.[41]

Another difference between the two technologies—cookies and DPI—is who uses each technology. The largest consumers of cookies have been Web sites, which gather information from consumers visiting their sites in order to produce relevant advertisements.[42] DPI, on the other hand, has been developed for and marketed to broadband providers or ISPs.[43] While a search engine only has access to information gathered while a consumer is using its Web site or service, an ISP has access to all of a consumer's Web activity and, because of this, has the ability to gather a more complete picture of the consumer's preferences.[44] Accordingly, the advertisements that an ISP has the ability to create are exceptionally relevant—"[a]nd the more relevant the ad, the higher the price a provider can charge an advertiser."[45] While information on exactly which ISPs are using the technology is unclear, marketing information available on a number of DPI Web sites has indicated that the technology is being used by ISPs.[46]

---

36. *Id.*

37. DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y 2001).

38. *Id.* at 503.

39. *See* Daniel B. Garrie, et. al, *The Legal Status of Spyware*, 59 FED. COMM. L.J. 157 (2006).

40. *See* Cookie Basics, http://computer.howstuffworks.com/cookie1.htm (last visited Apr. 7, 2010).

41. *See* Memorandum, *supra* note 5, at 5.

42. *See* DoubleClick, 154 F. Supp. 2d at 503-04; RUANE, *supra* note 5, at 2.

43. Memorandum, *supra* note 5, at 3.

44. *See id.*

45. *Id.*

46. Phorm, About Us, http://www.phorm.com/about/ (last visited Apr. 7, 2010) ("Phorm is a global personalisation technology company that makes content and advertising more relevant. Phorm's innovative platform preserves user privacy and delivers a more

E. The Courts—Applying Cookie Precedents

At this time, no actions brought against DPI companies have been decided in the United States. In November 2008, a class action filed in the U.S. District Court for the Northern District of California alleged that the partnership between NebuAd and various ISPs had breached the Electronic Communications Privacy Act of 1986 (ECPA), the Federal Computer Fraud and Abuse Act (CFAA), and two California laws.[47] The district court dismissed the suit in October 2009 after finding that the California courts lacked adequate jurisdiction.[48] In December 2009, Wide Open West (WOW!) was also sued in a class action in Illinois for its collaboration with NebuAd.[49] While a decision has yet to be issued in the WOW! litigation, it is likely that the court will analyze this class action by looking to two earlier cases. Those cases, *In re DoubleClick* and *In re Pharmatrak*, both apply federal statutory law to the use of cookies by Web companies that provide behavioral advertising systems. The results in the two cases are different, but the facts are distinguishable.

1. The *DoubleClick* Litigation

Some litigation has arisen surrounding the use of cookies on the Internet. The leading case in this area of law dealt with the company DoubleClick. DoubleClick used cookies and a four-step acquisition process to gather information about Web site visitors. It then worked with partners to provide behavioral advertising on affiliated Web sites using that

---

interesting online experience. Phorm's partners include leading Internet Service Providers (ISPs), publishers, ad networks, advertisers and agencies."); *see also* Statement of Alissa Cooper, *supra* note 8, at 14:

> The two most prominent ad networks engaged in this practice are NebuAd in the United States and Phorm in the UK. Charter Communications, a cable broadband ISP, recently announced—and then delayed—a plan to conduct trials of the NebuAd behavioral advertising technology. Several other ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq and Knology also announced plans with NebuAd to trial or deploy its behavioral advertising technology. Although a number of these ISPs have put their plans on hold in the wake of a firestorm of criticism, NebuAd continues to work with U.S. ISPs and seek new ISP partners. Phorm, which originally announced deals with three of the UK's largest ISPs and has sought partnerships with U.S. ISPs, is also now encountering hesitation from some of its UK partners.

47. Class Action Complaint at 3, Valentine v. NebuAd, Inc., No. 08 Civ. 5113 (N.D.Cal. Nov. 10, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (access PDF document through link labeled "download pdf").

48. Wendy Davis, *Judge Dismisses Case Against ISPs that Worked with Closed NebuAd*, MEDIAPOST NEWS, Oct. 12, 2009, http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=115259.

49. Wendy Davis, *New Lawsuit Says ISP Installed 'Spyware,' Misled Congress*, MEDIAPOST NEWS, Dec. 13, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=118994.

information.[50] The first step required an Internet user to direct his or her browser to a Web site that utilized DoubleClick technology.[51] Next, the Web site responded to the user with the basic content of the site.[52] Third, the user's computer asked the Web site for advertisements to fill in the blank banners.[53] If the individual had previously visited the Web site, the user would already have a cookie installed on his or her hard drive, and that cookie would communicate with a third-party advertising site (in this case, DoubleClick) to discover the user's preferences and fill in the advertising banners.[54] If the user had not previously visited the site, a cookie would download and begin to observe preferences. To complete the process, DoubleClick identified the cookie and then personalized advertisements based on the information associated with that cookie.[55] The result was a personalized, user-specific site.[56]

DoubleClick became involved in litigation when consumers filed suit in 2001, claiming that DoubleClick's information-gathering practices violated U.S. privacy law. The 2001 case was brought in the Southern District of New York, which held that using cookies to gather information for behavioral advertisements did not violate U.S. privacy law.[57] Before arriving at that conclusion, the court reviewed the plaintiffs' three federal, privacy law claims. Those claims included violations of Title II of the ECPA, the Federal Wiretap Act, and the CFAA.[58]

The plaintiffs' first claim accused DoubleClick of violating Title II of the ECPA, which "creates both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission."[59] Plaintiffs claimed that DoubleClick's action of gathering information from their computers via cookies constituted unauthorized access under Title II, Part A.[60] That section establishes that conduct in violation of the statute occurs when,

> [e]xcept as provided in subsection (c) of this section[,] whoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access

---

50. DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y 2001).
51. *Id.*; *see also* RUANE, *supra* note 5, at 1-2.
52. *DoubleClick*, 154 F. Supp. 2d at 502-03.
53. *Id*. at 503.
54. *Id.* at 503-04.
55. *Id.* at 503.
56. *Id.* at 503-04.
57. *DoubleClick*, 154 F. Supp. 2d at 500.
58. *Id.*
59. *Id.* at 507.
60. *Id.*

> to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . .[61]

In response to the complaint, the court held that DoubleClick's actions were in violation of Part A; however, it said that DoubleClick was not liable because its actions fell under an exception.[62] That exception states that "this section does not apply with respect to conduct authorized . . . (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user."[63] The court based its holding on a three-part analysis:

> (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites "users" of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick sufficient authorization to access plaintiff's stored communications "intended for" those Web sites?[64]

The court said that the relevant electronic communications service in this case was the Internet access and that the "users" were the Web sites under the ECPA.[65] Furthermore, the court said that DoubleClick-affiliated Web sites had received authorization to access plaintiffs information when the plaintiffs directed searches toward the DoubleClick sites.[66] The court said that "because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all 'intended for' those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access."[67]

Second, plaintiffs claimed DoubleClick violated the Federal Wiretap Act.[68] The Wiretap Act provides for criminal and civil rights of action when a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication."[69] Similar to the first claim, the court found that DoubleClick's activity violated the provision but fell under an exception.[70] The exception allows interceptions to be made when consent has been

---

61. *Id.* (quoting ECPA Title II, 18 U.S.C. § 2701 (2006)).

62. *Id.* at 507-09.

63. *DoubleClick*, 154 F. Supp. 2d at 507 (quoting ECPA Title II, 18 U.S.C. § 2701 (2006)).

64. *Id.* at 508.

65. *Id.* at 508-509.

66. *Id.* at 510.

67. *Id.* at 511. For full background information on GET, POST, and GIF cookie submissions, see id. at 504, stating that "GET information is submitted as part of a Web site's address or 'URL'"; "Users submit POST information when they fill-in multiple blank fields on a web-page"; and "GIF tags are the size of a single pixel and are invisible to users" and are placed on user computers when users visit "affiliated Web sites."

68. *Id.* at 514.

69. *DoubleClick*, 154 F. Supp. 2d at 514 (quoting the Federal Wiretap Act, 18 U.S.C. § 2511 (2006)).

70. *Id.*

given.[71]

Third, plaintiffs claimed DoubleClick violated the CFAA.[72] The CFAA provides a civil right of action when damages result in "any impairment to the integrity or availability of data, a program, a system, or information that—(A) *causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals*."[73] The court held that plaintiffs' losses did not result in $5,000 in damages.[74]

2. The *Pharmatrak* Litigation

In another case, *In re Pharmatrak*, the court again dealt with the acquisition of personal information by cookies. Unlike *DoubleClick*, however, the First Circuit Court of Appeals held that the use of cookies was illegal under the ECPA because, in this case, consent was not present.[75] The court held Pharmatrak liable for acquiring information for behavioral advertising profiles when customers visited affiliated pharmaceutical Web sites because the pharmaceutical companies were not aware of the site's ability to acquire information on users.[76] The First Circuit distinguished this case from the *DoubleClick* litigation because while DoubleClick Web sites had contracted for the express purpose of launching personal profiles, the *Pharmatrak* pharmaceutical companies did not believe that they had consented to the acquisition of consumers' personal information by Pharmatrak.[77] Because of this difference, the court held that Pharmatrak failed to meet the consent exemption that had previously been the basis of the *DoubleClick* holding.[78]

DPI technology presents greater privacy concerns than the cookies in *DoubleClick* and *Pharmatrak* because of the amount of user information available through DPI. Unlike a cookie, which sits dormant on the hard drive of a computer until an Internet user accesses a specific Web site associated with that cookie, DPI technology is able to copy all information that a consumer inputs into any Web site on the Internet at any time. This important difference is the root of new fears that online privacy rights may be at risk. Skeptics believe that DPI technology, if partnered with ISPs, could result in network degradation for certain users or in proprietary use

---

71. *Id.* at 514-15.

72. *Id.* at 519.

73. *Id.* at 520 (quoting the Computer Fraud and Abuse Act of 1996, 18 U.S.C. § 1030(e)(8)) (emphasis in original).

74. *Id.* at 523.

75. Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

76. *Id.* at 20.

77. *Id.*

78. *Id.* at 20-23.

of personal information.[79]

3. Beyond Cookies—The Status of DPI Litigation Today

With regard to the current class action in California, it is likely that the court will apply some combination of the *DoubleClick* and the *Pharmatrak* holdings. In applying those decisions, however, the court will likely focus on the differences between cookie technology and DPI. The differences will make a direct application of the case law difficult. If the court finds that the company acted for the express purpose of creating behavioral advertising profiles, it is likely that an analysis similar to the one in *DoubleClick* would be applied. If directly applied, *DoubleClick*'s precedent would place companies that agree to develop advertisement profiles under the consent exemptions present in the ECPA and the Federal Wiretap Act.[80] If applied in part, the most significant modification to the holding will likely appear in how the court analyzes consent.

a. Who Is Eligible To Consent?

Unlike in *DoubleClick*, the party conducting DPI profiling is not a user or a "party to the communication" like the Web site was in *DoubleClick*.[81] Instead, the DPI service provider is a third party with whom the ISP contracts to gather user information. Thus, the user does not seek out the party who is using DPI. Instead, the ISP—the underlying service that allows for the communication—seeks out the DPI party. This difference creates a dilemma as to who is eligible to consent because the user is not making an affirmative choice to seek out the DPI provider.

While this issue has yet to be adjudicated (or clarified by statute), government lawyers have signaled that, due to the difference in the parties

---

79. *ISP Targeting Hubbub Ignores Web Giants' Tracking, House Telecom Hears*, COMM. DAILY, July 18, 2008 (quoting Subcommittee Chairman Edward Markey (D-Mass.): "'Consumers deserve, at the least, at the minimum, one clear, conspicuous notice' of what DPI entails and 'no monitoring or interception' of their traffic if they decline.").

80. DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y 2001).

81. Memorandum, *supra* note 5, at 6; *DoubleClick*, 154 F. Supp. 2d at 508-09 (discussing "users" by citing 18 U.S.C. § 2510(13): "The ECPA defines a 'user' as 'any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use.' . . . On first reading, the DoubleClick-affiliated Web sites appear to be users—they are (1) 'entities' that (2) use Internet access and (3) are authorized to use Internet access by the ISPs to which they subscribe"). *Id*. at 514 (quoting the Federal Wiretap Act: "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception"); also stating that "[a]s a preliminary matter, we find that the DoubleClick-affiliated Web sites are 'parties to the communication[s]' from plaintiffs and have given sufficient consent to DoubleClick to intercept them.").

that are involved when DPI is used, the consent exception likely cannot apply to the ISP in the same way that it applied to the Web sites in *DoubleClick*.[82] Instead, in order for the exception to apply, the individual consumer must provide consent to the ISP in order for that ISP to use DPI to collect information.[83]

b. What Constitutes Consent?

In addition to the issue of who is eligible to consent, the issue of what constitutes consent is also an issue of contention.[84] At the beginning of the debate, companies that were in favor of using DPI services believed that adequate consent was available through an opt-out structure;[85] meanwhile, privacy and security advocates did not believe that an opt-out regime provided adequate protection for consumers, preferring instead an opt-in regime.[86]

Opt-out and opt-in structures for affirmative consent require different actions on the part of the consumer. Under an opt-out structure, a consumer is notified that "his or her ISP has agreed to allow an online advertiser to track that person's online activity"; the consumer is then notified that, if he or she does not want to participate, he or she must notify the ISP or DPI provider.[87] If the consumer provides no response, then his or her consent is

---

82. RUANE, *supra* note 5, at 5-7.

83. *Id.* at 5-8; *see also* 18 U.S.C. § 2511 (2006).

84. RUANE, *supra* note 5, at 5-8.

85. *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong., at 4-5 (2008) (testimony of Bob Dykes, CEO NebuAd), *available at* http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Dykes-testimony.pdf (hereinafter Testimony of Bob Dykes); *see also* Phorm Inc.: Industry Privacy, http://privacy.phorm.com/ industry_standards.php (last visited Apr. 7, 2010).

86. Jim Puzzanghera, *Opt-in Rule Sought for Web Tracking*, L.A. TIMES, July 18, 2008, at C-3 (quoting Chairman Edward Markey (D-Mass.): "That's basically saying silence is consent and as a result you can do whatever you want with their information. . . . I don't think, unless you've got clear affirmative permission, that you should be able to take this incredible leap into the breaching of the privacy of Americans." The article continued by saying, "Markey said such an opt-in requirement should be included in online privacy legislation he is working on."). *See also What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2008) (formal statement of Chairman John Dingell (D-Mich.)), *available at* http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1264&catid=18:platforms&Itemid=58 (discussing Embarq's use of DPI technology saying "[n]ot only did Embarq fail to give its subscribers a chance to opt in to the tracking, but it did not directly notify affected customers that they had a chance to opt out. I find the notion that a broadband provider would implement such tracking with no real notice to the customer to be deeply troubling.") (hereinafter formal statement of Chairman Dingell).

87. RUANE, *supra* note 5, at 8.

inferred.[88] Companies like NebuAd and the UK's Phorm operated under an opt-out regime.[89] An opt-in structure conversely requires consumer consent before the collection of information may begin.[90] A consumer who does not respond to the consent request would not allow the DPI company to collect information. Some have suggested that, in executing an opt-in structure, a pop-up box would appear on an Internet user's computer screen and a consumer would be required to choose to allow information collection to occur before it could begin.[91]

Since the fall of NebuAd and increased congressional and media pressure on companies to provide high levels of privacy and transparency, the opt-in debate has changed. Companies have signaled that they will not conduct behavioral advertisement without some level of opt-in or "engaged" consent.[92]

F. A Proactive Approach—Regulatory Vehicles Applying to Behavioral Advertising

1. The FTC—A Light Regulatory Touch

Due to the lack of jurisprudence dealing with DPI technology and the confusion in determining what the appropriate consent standard should be in order to best utilize the technology, the FTC began looking at the concerns of privacy advocates in a series of 2006 hearings and 2007 town-hall meetings.[93] In response to those events, staff from the FTC released a set of four broad, self-regulatory principles that dealt with behavioral advertising.[94] The four principles included (1) "transparency and consumer control," (2) "reasonable security and limited data retention for consumer data," (3) "affirmative express consent for material changes to existing privacy promises," and (4) "affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising."[95]

---

88. *See id.*

89. *See* Phorm Inc.: Industry Privacy, *supra* note 85.

90. RUANE, *supra* note 5, at 7-8.

91. *ISP Targeting Hubbub Ignores Web Giants' Tracking, House Telecom Hears*, *supra* note 79.

92. Preliminary Transcript, *Hearing on Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech. and the Internet of the H. Comm. on Energy and Commerce*, at 90-92, 111th CONG., Apr. 23, 2009, *available at* http://energycommerce.house.gov/Press_111/20090423/transcript_20090423_ti.pdf [hereinafter *Consumer Privacy Hearing Preliminary Transcript*].

93. Press Release, FTC, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm.

94. *Id.*

95. Statement of the Bureau of Consumer Protection Proposing Governing Principles for Online Behavioral Advertisement, FTC, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, at 3-6 (Dec. 20, 2007), *available*

The FTC sought comment from the industry on how these principles would affect the Internet environment.[96] The industry responded with mixed reactions. Internet giant Google was one of sixty-three respondents. It worried that the definition of behavioral advertising was too broad and would include both personally identifiable and non-personally identifiable information.[97] In addition, AT&T endorsed the principles, but encouraged the FTC to ensure that they were applied in a neutral way.[98] The Consumer Federation of America did not find the principles to be satisfactory and commented as follows:

> [W]e would like to state at the onset that consumers cannot be adequately protected by self-regulatory principles and general FTC enforcement powers.
>
> The evidence presented at the Town Hall meetings not only demonstrates the failure of the current voluntary approach but the inevitable inability of poorly defined principles to protect the public. There is a deep-seeded failure in the online advertising/marketing space that cannot be addressed by half measures.[99]

In sum, eighty-seven parties, including representatives from business, academia, advocacy groups, and the general public, commented in the proceeding's sixty-three filings.[100] Following the comment period, the FTC released revised principles in February 2009. The revised principles were modified to recognize the concerns of many of the commenting parties.

The modified principles begin with a new definition for behavioral advertising:

> [O]nline behavioral advertising means the tracking of a consumer's online activities ***over time***—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. ***This definition is not intended to include "first party" advertising, where***

---

at www.ftc.gov/os/2007/12/P859900stmt.pdf.

96. FTC Press Release, *supra* note 93 (stating that "[b]ecause online advertising supports free Web content and other benefits, the choice by consumers not to participate in behavioral advertising could reduce the availability of these benefits").

97. Letter from Alan Davidson, Senior Policy Counsel and Head of U.S. Public Policy, Google Inc., to Jessica Rich, FTC (Apr. 4, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080404google.pdf; *see generally* Public Comments on the FTC Self-Regulatory Principles, http://www.ftc.gov/os/comments/behavioraladprinciples/index.shtm (last visited Apr. 7, 2010).

98. Letter from Bruce R. Byrd, Vice President and General Counsel, AT&T, to Office of the Secretary, FTC (Apr. 11, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080411at&t.pdf.

99. Letter from Consumer Federation of America and Consumer Union, to Donald S. Clark, Secretary, FTC 1-2 (Apr. 11, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080411cfacu.pdf.

100. FTC, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

> ***no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query.***[101]

As the definition signals, "behavioral advertising" here relates specifically to Web services that track consumer Web choices on a variety of sites and use a third party to gather the information. The definition clearly includes DPI technology when that technology is partnered with an ISP and tracks consumer preferences across the Web.

The main principles in the revised FTC report remained the same in the February report.[102] However, the explanations of each principle became more detailed. In conjunction with the first principle, "Transparency and Consumer Control," the FTC stated that Web sites that collect information should "provide a clear, concise, consumer-friendly, and prominent statement" that data are being collected for advertising purposes and that consumers can opt out of the service.[103] The FTC suggests that companies showing this type of message should provide easy ways to opt out. Additionally, the FTC suggests that in nontraditional Web site–based collection—presumably the collection of information over an ISP system—notification be present to provide context for that type of information gathering.[104]

In the second principle, the FTC discusses "Reasonable Security, and Limited Data Retention, for Consumer Data."[105] Here, the FTC suggests that companies should employ "reasonable security measures" for compiled data.[106] The FTC suggests that these security measures should be proportionate to the apparent risk.[107] Additionally, the FTC requests that companies hold information for the maximum amount of time needed.[108]

The third principle is "Affirmative Express Consent for Material Changes to Existing Privacy Promises."[109] This principle suggests that users receive consumer consent before information is used, even when the applicable privacy policy does not require notification.[110] The FTC's policy would thus affect data collection retroactively and proactively. Notification of use under this principle likely would require notification under the standards signaled in the first principle.

---

101. *Id.* at 46 (emphasis in original).
102. *Id.* at 46-47.
103. *Id.* at 46.
104. *See id.*
105. *Id.*
106. *Id.* at 46-47.
107. *Id.* at 47.
108. *Id.*
109. *Id.*
110. *Id.*

The fourth and final principle, "Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising,"[111] seeks to guard against the release of personal information that may connect a consumer to potentially problematic or "sensitive" information. While there is not a complete definition of what constitutes "sensitive information," it is accepted that this type of information includes "financial data, data about children, health information, precise geographic location information, and Social Security numbers."[112] Due to the lack of clarity here, the FTC noted its desire to work to develop better definitions in the future.[113] Affirmative express consent is suggested for this type of information. The FTC principles give a limited definition of what the FTC considers to constitute affirmative express consent and signaled that it requires action on the part of the consumer, stating that "pre-checked boxes or disclosures that are buried in a privacy policy or a uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer's 'affirmative express consent.'"[114]

The FTC principles are self-regulatory in design and thus do not have an enforcement mechanism. The FTC has recognized, however, that, if the self-regulatory nature of the principles is not enough to affect the industry, then more work in the future may be warranted.[115]

2. Congress—A Heavy Regulatory Approach

In addition to the work that the FTC completed, members of Congress pledged to pass legislation to clarify privacy rights online.[116] Beginning in

---

111. *Id.*

112. *Id.* at 44.

113. *See id.*

114. *Id.* at 44 n.77.

115. *Id.* at 48, stating as follows:

> Looking forward, the Commission will continue to monitor the marketplace closely so that it can take appropriate action to protect consumers. During the next year, Commission staff will evaluate the development of self-regulatory programs and the extent to which they serve the essential goals set out in the Principles; conduct investigations, where appropriate, of practices in the industry to determine if they violate Section 5 of the FTC Act or other laws; meet with companies, consumer groups, trade associations, and other stakeholders to keep pace with changes; and look for opportunities to use the Commission's research tools to study developments in this area.

Id.

116. *See, e.g.*, Boucher, *supra* note 4. Boucher notes the following:

> I want to promote greater use of the Internet by assuring Internet users a high degree of privacy protection, including transparency about the collection, use and sharing of information about them, and giving them control over that collection, use and sharing. Consumers are entitled to some baseline protections in the online space. If someone does not want a Web site he visits to use information it collects to deliver ads to him, he should be able to opt out of that use. A consumer also has a reasonable expectation that a Web site he visits will not be sharing his

the summer of 2008, the House Energy and Commerce Committee's Subcommittee on Communications, Technology, and the Internet and the Senate Commerce Committee held hearings related to online privacy. DPI technology was of special focus in both houses where the then-CEO of NebuAd testified about the technology.[117] Former Subcommittee Chairman Edward Markey (D-Mass.) took a firm stance on acquisition of personally identifiable information on the Internet and was quoted in *Communications Daily*, saying, "[t]his is only going to become an escalating subject" for the committee.[118] Markey also expressed his opinion that an opt-out regime was not appropriate and that an opt-in regulation for use of DPI was the only appropriate action.[119]

In addition to hearings, the members of the 110th Congress took a strong stance on DPI regulation.[120] In July 2008, Representatives Markey, Barton, and Dingell wrote a letter to Embarq, suggesting that its use of DPI technology may not be legal.[121] Additionally, Charter Communications

---

> information with unrelated third parties. Accordingly, if a Web site wants to provide information to an unrelated third party, it should procure that Internet user's opt-in consent. This structure should not prove burdensome for Internet-based businesses that rely on targeted advertising and is in line with the practices of reputable service providers today. More importantly, by giving Internet users a greater confidence that they have control over the collection and use of information about them by Web sites, the privacy guarantees will encourage greater levels of general Internet usage and e-commerce, benefiting not only consumers, but also the companies that transact business online and our nation's economy. I will be offering bipartisan legislation with Congressman Stearns to provide privacy assurances soon.

Id. See also ISP Targeting Hubbub Ignores Web Giants' Tracking, House Telecom Hears, *supra* note 79.

117. *ISP Targeting Hubbub Ignores Web Giants' Tracking, House Telecom Hears*, *supra* note 79.

118. *Id.*

119. *Id.* (transcribing the dialogue between Markey and Dykes: Markey sparred with NebuAd's Dykes over his refusal to say whether he supports opt-in. "You've got to get the consumer to say 'yes,'" Markey said, calling NebuAd "Google times a hundred." Dykes said: "You're forcing me into a 'have you stopped beating your wife?' question," to which Markey replied the actual question was "have you stopped beating your customer?" NebuAd doesn't track users that "we are convinced don't want to be tracked," Dykes said. "That's basically saying that silence is consent," Markey said, an "incredible leap" toward saying the mailman can open any letter.").

120. While Markey has remained on the subcommittee in the 111th Congress, Boucher of Virginia took over as Subcommittee Chair. At the time of transition, it was unclear how this change in leadership would modify the goals of the subcommittee in privacy legislation, which Markey has championed before. Since his chairmanship began at the start of 2009, Boucher has focused on privacy issues. *See* 154 CONG. REC. D915, *supra* note 1; 155 CONG. REC. D1333, *supra* note 1; 155 CONG. REC. D432, *supra* note 1. He has indicated that his priorities for the second session of the 111th Congress include privacy issues. *See* Boucher, *supra* note 4.

121. Formal statement of Chairman Dingell, *supra* note 86. *See also* Letter from David W. Zesiger, Senior Vice President, Embarq, to Representatives Dingell, Barton, and Markey

withdrew partnerships with NebuAd after a similar reaction by congressional leaders.[122] As a result, the CEO of NebuAd resigned and the company modified its business plan,[123] eventually closing its doors in 2009.[124]

Maintaining its commitment to online privacy regulation, the 111th Congress continued its review of DPI technology. Beginning in April 2009, Subcommittee Chairman Boucher dedicated a hearing to the current state of DPI technology in the United States.[125] The hearing confirmed that while none of the witnesses were using behavioral advertising,[126] interest existed to develop programs to utilize the technology for advertising purposes. AT&T witness Dorothy Attwood stated in her written testimony:

> The first thing that AT&T is doing to address the challenge of

---

(July 21, 2008), *available at* http://www.energycommerce.house.gov/Press_110/Embarq-Response.2.pdf.

122. *NebuAd Loses CEO, Pursues Less Controversial Pastures*, MARKETING VOX, Sept. 4, 2008, http://www.marketingvox.com/nebuad-loses-ceo-pursues-less-controversial-pastures-040764/. *See also* Posting of Saul Hansen to Bits blog, http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/?partner=rssnyt&emc=rss (May 14, 2008, 8:40 EST).

123. *See* Nate Anderson, *NebuAd Loses CEO, Business Model in Wake of Tracking Furor*, ARS TECHNICA, Sept. 5, 2008, http://arstechnica.com/news.ars/post/20080905-nebuad-loses-ceo-business-model-in-wake-of-tracking-furor.html.

124. NebuAd, Inc.: Private Company Information—Business Week, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=29980558 (last visited Apr. 7, 2010) (stating that "[a]s of 2009, NebuAd, Inc. went out of business. NebuAd, Inc., an online media company, offers online advertising solutions. The company's behavioral advertising solutions help advertisers, publishers, and service providers. NebuAd, Inc. was founded in 2006 and is based in Redwood City, California with additional offices in the United Kingdom").

125. 155 CONG. REC. D432, *supra* note 1. The hearing featured a witness list that included: Ben Scott, Policy Director, Free Press; Leslie Harris, President and CEO, Center for Democracy and Technology; Kyle McSlarrow, President and CEO, National Cable and Telecommunications Association; Dorothy Attwood, Chief Privacy Officer and Senior Vice President, Public Policy, AT&T Services, Inc.; Brian R. Knapp, Chief Operating Officer, Loopt, Inc.; Marc Rotenberg, Executive Director, The Electronic Privacy Information Center; and Richard Bennett, Publisher, BroadbandPolitics.com. Communications Networks and Consumer Privacy: Recent Developments, http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1590:energy-and-commerce subcommittee-hearing-on-communications-networks-and-consumer-privacy-recent-developments&catid=134:subcommittee-on-communications-technology-and-the-internet&Itemid=74 (last visited Apr. 7, 2010).

126. During the Hearing on Communications, Networks, and Consumer Privacy, Chairman Boucher said:

> And while I am certain that no one appearing on the panel today uses DPI in this manner, our discussion today of the capabilities of the technology and the extent of its current deployment, any projection that could be made about its anticipated schedule and path of deployment and the uses to which that technology is currently being put will give us as a subcommittee a better understanding of where to draw the lines between permissible and impermissible uses.

Consumer Privacy Hearing Preliminary Transcript, *supra* note 92, at 5.

> behavioral advertising—its promise and potential pitfalls—is to avoid thoughtlessly lurching into this realm without proper due diligence. We will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to engage consumers and ensure the protection of, and ultimate consumer control over, consumer information. . . . If AT&T deploys these technologies and processes, it will do so the right way.[127]

Others like Kyle McSlarrow from NCTA and Dorothy Attwood indicated that legislation should be technology-neutral and not focus on one technology and how it could potentially be used.[128] NCTA also stated that legislation was not needed and encouraged self-regulation.[129] Other panelists expressed views that DPI presented substantial concerns that the committee needs to address in legislation.[130] While some members of the committee echoed these concerns,[131] others said that it was important not to forget about the benefits that the technology brings to consumers.[132] In general, panelists agreed that consent and transparency were important and that consumers should be able to opt in before using the service.[133]

The House Energy and Commerce Committee also held a joint hearing with the Subcommittees of Commerce, Trade and Consumer Protection and the Subcommittee on Communications, Technology and the Internet dealing with online and offline advertisement practices.[134] The

---

127. *Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech. and the Internet of the H. Comm. on Energy*, 111th Cong. (2009) (Written Statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T Inc.), *available at* http://energycommerce.house.gov/Press_111/20090423/testimony_attwood.pdf [hereinafter Written Statement of Dorothy Attwood].

128. *Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech., and the Internet of the H. Committee on Energy and Commerce*, 111th Cong. (2009) (Statement of Kyle McSlarrow, President and CEO, National Cable and Television Association) at 2-3, *available* at http://energycommerce.house.gov/Press_111/20090423/testimony_mcslarrow.pdf (stating "we would respectfully suggest that focusing exclusively on one particular technology- and how it *might* be misued - risks obscuring an informed and reasonable discussion of online privacy when there are unlimited numbers of technologies and situations that could by hypothesized.") [hereinafter Written Statement of Kyle McSlarrow]; *id.* at 6; Written Statement of Dorothy Attwood, *supra* note 127, at 6.

129. *Consumer Privacy Hearing Preliminary Transcript*, *supra* note 92, at 38.

130. *Id.* at 29-30, 43, 52-56 (transcribing testimony by panelists Harris, Roteberg, and Scott).

131. *Id.* at 4-5, 12-13, 15 (transcribing statements made by Chairman Rick Boucher, Representative Anna Eshoo, and Representative Mary Bono Mack).

132. *See id.* at 9, 19, 22-23 (transcribing statements made by Ranking Member Cliff Stearns, Representative George Radanovich, and Representative Marsha Blackburn).

133. *See id.*

134. CONG. REC. D1354 (daily ed. Nov. 18, 2009) (notice of *Committee Meeting, H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer*

hearing took place in November 2009 and discussed privacy issues beyond DPI, including offline issues of privacy. While DPI was an issue, the committee focused on a wide array of privacy issues, including significant time on Wal-Mart's tracking actions and general advertising practices.[135] Yet while the committee indicated in this hearing that privacy legislation is close approaching,[136] the press following the hearing voiced its doubts and quoted FCC aide Sherrese Smith as saying, "[o]ne of the biggest impediments to a bill going through is the plight of media companies and their reputations with readers."[137] Smith's comments referenced a recent study by the Berkeley Center for Law and Technology and the Annenberg School for Communication at the University of Pennsylvania that states that the public's attitude toward behavioral advertising is not favorable and support for rules limiting behavioral advertising is high.[138] Yet, she said that when consumers recognize that passing rules to limit behavioral advertising will impact services that consumers know (like the *Washington Post* and the *New York Times*), support for regulation weakens.[139] At the time of publication, no draft legislation had been released in the House or in the Senate.

3. Across the Pond—A Different Approach

While Congressional leaders may believe that DPI presents more harms than benefits, others believe the technology allows for a premium online experience.[140] The British response to DPI, while still cautious, was, at the start, more accepting. In the United Kingdom, British Telecom (BT) worked with Phorm in early 2008 to complete a trial using Phorm's DPI

Protection and the Subcomm. on Comm., Tech., and the Internet joint hearing entitled *Exploring the Offline and Online Collection and Use of Consumer Information*).

135. Preliminary Transcript, *Exploring the Offline and Online Collection and Use of Consumer Information Hearing before the Subcomm. on Commerce, Trade and Consumer Protection and the Subcomm. on Comm., Tech., and the Internet of the H. Energy and Commerce Comm.*, 111th CONG., Nov. 19, 2009, *available at* http://energycommerce.house.gov/Press_111/20091119/transcript_11192009_cti.pdf.

136. *See id.*

137. Greg Piper, *Behavioral Ad Bill Unlikely to Get Through Congress*, COMM. DAILY, Nov. 13, 2009, at 10, *available at* 2009 WLNR 23180769.

138. *Id.* (stating "[t]he survey by the Berkeley Center for Law & Technology and the Annenberg School for Communication at the University of Pennsylvania found two-thirds of adults don't want targeted ads, and a slight majority of those 18-24 feel the same").

139. *Id.*

140. *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Science and Transportation.*, 110th Cong., at 7 (2008) (statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T Inc.) ("Indeed, . . . behavioral advertising could prove quite valuable to consumers and could dramatically improve their online experiences."); *BT Gives Phorm's Behavioral Ad Model Another Go*, MARKETING VOX, Sept. 29, 2008, http://www.marketingvox.com/bt-gives-phorms-behavioral-ad-model-another-go-041214.

technology to provide a more personalized experience online.[141] The Phorm technology provided behavioral advertising through a proprietary program called Webwise.[142] The service, which is conducted in partnership with ISPs, does not store PII; rather, it assigns random numbers to each user's computer within the Webwise program.[143] The program blocks sensitive sites like Webmail and other topics like "pornography, medical, gambling, tobacco, or alcohol" from user profiles.[144] User profiles are compiled with material covering broad subjects like travel or finance.[145]

In testing the technology on the BT network, the trial reached out to approximately 10,000 consumers in the United Kingdom and provided them with the option to opt into the trial for a period of several weeks.[146] The trial used a "special webpage" to invite consumers to join the trial, read the applicable terms of service, and opt in or out for the Webwise program.[147]

The BT-Phorm partnership offered two services for consumers to test during the trial period. First, the trial tested a custom advertisement service to consumers.[148] The advertisements were based on consumer preferences that the technology detected through the data acquired during online activity. To acquire that information, Phorm's technology intercepted Web activity that took place over the BT network and matched "categories of browsing activity with advertising."[149] Second, the technology provided consumers with an online antifraud protection service.[150] The service works with a "blacklist" of Web sites to protect consumers against phishing scams and virus activity.[151] While using the service, any consumer who traveled to

---

141. Press Release, Phorm, Inc., BT Trial Update (Dec. 15, 2008), *available at* http://investing.thisismoney.co.uk/security.cgi?csi=109833&action=news&story_id=2510703&rns=1.

142. BT Webwise, http://www2.bt.com/static/i/btretail/webwise/ (last visited Apr. 7, 2010).

143. PHORM FINAL PRIVACY IMPACT ANALYSIS, 80/20 THINKING, at 21, *available at* http://www.phorm.com/technology/privacy_assessments.html.

144. *Id.* at 20.

145. Webwise: Privacy: No Personal Information Collected, http://www.webwise.com/privacy/no-personal-info.html (last visited Apr. 7, 2010).

146. Chris Williams, *BT's Third Phorm Trial Starts Tomorrow*, THE REGISTER, Sept. 28, 2008, *available at* http://www.theregister.co.uk/2008/09/29/bt_phorm_trial_go/. *See also* AMG Questions 2008, http://www.btplc.com/Sharesandperformance/AGMs/AGM2008/Questions.htm (last visited Apr. 7, 2010).

147. Williams, *supra* note 146 (showing samples of the invitation screen offered as part of the BT-Webwise trial).

148. BT Webwise, *supra* note 142.

149. Webwise: How It Works, http://www.webwise.com/how-it-works/how-it-works.html (last visited Apr. 7, 2010).

150. BT Webwise, *supra* note 142. *See also* Webwise Features: Online Fraud Protection, http://www.webwise.com/features/anti-fraud.html (last visited Apr. 7, 2010).

151. *See* BT Webwise, *supra* note 142; *see also* Webwise: How It Works, *supra* note

one of the untrustworthy blacklisted Web sites would receive a warning page suggesting that the consumer end its communication with the suspected site.[152] The service was designed to complement existing virus-protection software and browser notification systems.[153]

Responses to the BT-Phorm Webwise trial were mixed. Similar to American critics, British critics have raised concerns that the program is too intrusive and violates user rights online.[154] The European Union has also raised concerns with the program, stating that it violates EU privacy law, but the UK Parliament, has been more accepting of the technology, finding that it comports with British law and policy.[155]

From the start, the 2008 Phorm-BT trial attempted to provide a transparent approach to what information the companies could collect and how they could secure it. Phorm took a major step in 2008 to ensure elevated data protection when it completed a privacy impact assessment (PIA). The assessment is a comprehensive report which included a "process whereby a project's potential privacy issues and risks are identified and examined from the perspectives all stakeholders, and a search is undertaken for ways to avoid or minimize privacy concerns."[156] The report suggests that Phorm's commitment to security makes its product safe for users.[157] It states that if an opt-out mechanism is used instead of an opt-in one, it must "use clear and ongoing notification, and minimal disruption" to consumers.[158] The PIA also cautions the company to realize that the perception of DPI is not positive at this point and that Phorm needs to take the public image of DPI seriously as it develops its product and establishes partnership agreements.[159] The report also commends the company for blocking over 1,000 Webmail sites,[160] encouraging industry best practices, and initiating a town hall for other companies in the sector.[161] The privacy

---

149.

152. *See supra* note 151.

153. Webwise Frequently Asked Questions, http://www.webwise.com/how-it-works/faq.html (last visited Apr. 7, 2010); BT Webwise, How It Works, (on file with the author).

154. *See* No DPI Home Page, www.nodpi.org (last visited Apr. 7, 2010).

155. Erica Herrero-Martinez, *Phorm, BT Consumer Tracking Platform Online by End of '09*, DOW JONES NEWSWIRES, Feb. 9, 2009 (stating "The European Commission previously voiced concern that Phorm's platform breaches consumer privacy directives, but the U.K. government has backed the company and said it is capable of operating lawfully and appropriately.").

156. Privacy Impact Assessment, 80/20 Thinking Analysis at 12 (2008), *available for download at* http://www.webwise.com/privacy/privacy_impact_report.html [hereinafter Privacy Impact Assessment].

157. *Id.* at 13.

158. *Id.* at 7.

159. *Id.* at 7.

160. *Id.* at 18.

161. *Id.* at 5.

analysis and schematic set up by Phorm presents a compelling argument that correct standards for online privacy can make DPI technology a benefit and not a problem.

Since the conclusion of the trial, BT has decided not to utilize the Webwise program because of its current priority to use resources for rollout of next generation services.[162] BT emphasized in its public statements, however, that its reason for stopping the trial is not due to the debate on privacy surrounding the service, and that it may deploy the product at a later time.[163] Interest for DPI technology in the United Kingdom has not been eliminated with the completion of the Webwise trial, and other major companies continue to be interested in the development of similar systems. Media reports have indicated that companies like TalkTalk and Virgin Communications are currently reviewing possible partnerships with DPI companies.[164]

III. IN SEARCH OF A REGULATORY MIDDLE GROUND

The regulation of DPI technology presents a difficult task for American lawmakers. Phorm's PIA Assessment was correct when it said that the "technology offers a high standard of privacy and data protection. However there continues to be a serious risk that the product will be perceived as invasive."[165] Like consumers in the United Kingdom, U.S. consumers do not want "Big Brother" snooping into their online communications. Nevertheless, citizens of both the United States and the United Kingdom, want the most innovative Internet experience. While the perception of DPI is less than perfect, the technology has the potential to bring significant benefits to Internet consumers.

A. Looking at the Benefits

While obvious benefits like more virus protection and better advertisements have been the consumer focus of companies pushing the technology, more relevant advertisements will result in discounts and offers for consumers who are more likely to benefit from those specials.[166] In

---

162. *See* BT Webwise, *supra* note 142. Tom Espiner, *BT Shelves Phorm Ad-Serving Technology: The British Telco Has Postponed Plans To Deploy Controversial Technology Targeting Online Ads to Customer Behavior, but TalkTalk and Virgin Still May*, BUS. WK., July 7, 2009, *available at* http://www.businessweek.com/globalbiz/content/jul2009/gb2009077_774630.htm.

163. Espiner, *supra* note 162 (stating "BT's decision to put Webwise on hold was not connected to customer concerns about the privacy of such a service, a spokesperson for the company told silicon.com sister site ZDNet UK."); *see also* BT Webwise, *supra* note 142.

164. *See id.*

165. Privacy Impact Assessment, *supra* note 156, at 8.

166. Tresa Baldas, *Advertiser Tracking of Web Surfing Brings Suits Class Action Filed; Guidelines Issued*, NAT'L L.J., Mar. 2, 2009, at 1, 22 (stating that Seyfarth Shaw Partner

addition to the advertising benefits for consumers, DPI provides the opportunity for the establishment of new revenue streams for ISPs, which could influence subscription rates and deployment statistics. Internet advertising revenue "grew to $23.4 billion in 2008, an increase of 10.6 percent from 2007."[167] For companies that are struggling to stay afloat in the current economy, more ISP revenue could aid in the deployment of Internet services to areas where the cost of infrastructure development is high. Accordingly, avoiding revenue stream limitations might help maintain or increase access to free services online. When it released its self-regulatory principles, the FTC signaled that the adoption of privacy regulations could potentially affect the ability of companies to provide the same breadth of free online services.[168]

DPI provides access to individualized advertisements in ways that are not malicious and do not slow down computers. The technology also may be used by ISPs to differentiate their companies in the market and to protect their infrastructure by providing heightened security and protection.

B. Looking Past the Perception in Search of a Solution

Instead of buying into the perception that DPI technology is dangerous, Congress must approach online privacy regulations realistically with its eyes open to the real effects that regulations could have on consumers and the Internet. Congressional actions in both the 110th and 111th Congresses conveyed a general negativity toward DPI, while conveying a favorable sentiment toward privacy legislation that could potentially close the door to future use of the technology completely. If Congress is serious about drafting privacy legislation to limit (or eliminate) the use of DPI, members of Congress should think comprehensively about how they will address the needs of their constituents both as consumers of the Internet and as private individuals interested in protecting their data. Congress must look at both sides of the argument. It must research what is being done abroad to understand the benefits that are seen by other countries like the United Kingdom.

1. A Clarification of Law

It is clear that there is a need for action on the part of lawmakers to

---

Bart Lazar "sees some benefits to behavioral advertising, such as consumers' ability to receive discounts and other information about products and services that they are interested in purchasing").

167. Stephanie Clifford, *Ad Sales up on Internet, but '08 Pace Was Slower*, N.Y. TIMES, Mar. 20, 2009, at B9.

168. FTC Press Release, *supra* note 93 ("Because online advertising supports free Web content and other benefits, the choice by consumers not to participate in behavioral advertising could reduce the availability of these benefits.").

clarify what judicial opinions and statutes apply to DPI technology. It will be important for Congress to clarify ambiguities that were not part of the *DoubleClick* and *Pharmatrak* decisions, like the issue dealing with consent. Clarification of these issues will give ISPs better notice of how to provide their consumers with the best online access. In doing this, Congress should clarify how provisions in the Electronic Privacy Act, the Federal Wiretap Act, and the Communications Act apply to ISPs that want to collect information for advertising profiles. At a minimum, clarification must designate the structure for consent (opt-in or opt-out) and the consenting party (the ISP or the user).

2. A Consent Regime

Regardless of the decision to use an opt-in or opt-out structure, Congress must leave the door open for companies to have a clear and easy way to obtain consent from consumers who want to use the service. The BT-Phorm trial used a method of obtaining opt-in consent that displayed an on-screen box before a session.[169] This is a good way to make sure consumers are aware of the service and can provide consent easily if they choose to participate. AT&T's approach—requiring consumers to be engaged in the consent process—is also a good start.[170] Additionally, consent preferences must be adjustable. If a consumer decides that he or she would like to join the program later, additional consent should follow an equally simple format. Finally, consent procedures should not be so limiting that companies find it impossible to operate a business or innovate.

3. A Review of International Approaches

Congress should also look at the pilot programs in the United Kingdom for ideas on how to establish best practices. Under the Webwise trial, Phorm suggested establishment of industry working groups to generate ideas on protection of information.[171] A similar working group in the United States would ensure that industry holds itself to the best standards and that a mandated approach does not stifle innovation. Additionally, Phorm developed its own best practices, which included easy access to its privacy policy, blocking over 1,000 Webmail addresses from the reach of its technology, and a serious attempt to make user profiles anonymous.[172] If Congress chooses to regulate behavioral advertising in the United States, it should look to these strategies and other industry strategies to create a safe-harbor provision for companies who act in good faith to

169. *See supra* note 147 and accompanying text.
170. *See Consumer Privacy Hearing Preliminary Transcript*, *supra* note 92, at 74-75.
171. Privacy Impact Assessment, *supra note* 156, at 6.
172. *Id.*

protect consumer information. As Marc Rotenberg, Executive Director of EPIC, said before the Subcommittee on Communications, Technology, and the Internet last spring, "no one agrees to a security breach."[173] A safe-harbor provision would not be mandatory, but would protect ISPs that strive to provide innovative DPI services to consumers by giving those service providers with a safeguarded way to offer DPI.

4. A Consistent Policy

Congress should also work to establish a consistent regulatory policy for ISPs and Web sites that are interested in providing behavioral advertising. Web site providers also gather information in bulk through search engines, free online e-mail accounts, and shopping services.[174] It would be foolish to forget this fact when establishing privacy rights. A comprehensive and neutral approach to regulation that is not limited to one type of technology will provide the best environment for growth and innovation online. It will also limit the number of loopholes that may cause favoritism of one technology over another. If Congress is serious about protecting online data, then it must recognize that a number of legitimate services collect data online. DPI is not the only technology that gathers—or will gather—large amounts of private information online. A flexible, light regulatory framework that provides general protection over information-gathering technologies and does not focus on one specific technology will serve to protect information while also preserving innovative ideas. Too strong of a regulation could stop companies from developing innovative services for fear that their investments may result in a negative return, similar to NebuAd. At the House hearing in April 2009, Loopt testified that it uses these type of technologies in its location-based services,[175] while NCTA President Kyle McSlarrow testified that other sectors of the communications industry plan to utilize similar technology to enhance consumer experiences (for example, set-top cable boxes and cable advertisements). Today, companies use behavioral advertising to offset the cost of services to online consumers.[176] In writing an expansive privacy framework, it is important for Congress to think about how a statute for DPI collection methods may result in unintended consequences for some of these free services—specifically with customer favorites like the free services available on sites such as Gmail, Facebook, or CNN.com.

---

173. *Consumer Privacy Hearing Preliminary Transcript*, *supra* note 92, at 103.

174. *See Consumer Privacy Hearing Preliminary Transcript*, *supra* note 92, at 79-80.

175. *See Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech. and the Internet of the H. Comm. on Energy and Commerce*, 111th CONG. (2009) (Statement of Brian R. Knapp, COO, Loopt), *available at* http://energycommerce.house.gov/Press_111/20090423/testimony_knapp.pdf.

176. *See* Written Statement of Kyle McSlarrow, *supra* note 128, at 4.

5. A Review of the Public Policy Hurdles

Most importantly, in deciding if and how to regulate, Congress should look at the consequences that different regulations may have on other important policy goals. In looking at DPI regulations, it is important for Congress to consider how behavioral advertising regulation may affect other uses of DPI technology, such as network management, CALEA compliance, and development of tiered-service pricing schematics. If DPI is regulated out of existence as a behavioral advertisement technology, it is likely that companies will not want to risk litigation by using it in other contexts either. The result could limit both potentially cost-saving options for Internet offerings and innovative consumer security services. DPI, like all other technologies, may be used for good or bad purposes. I do not dispute that some form of privacy regulation framework is needed to deal with online privacy concerns, but that framework should be general, apply to a variety of technologies, and encourage innovation on the Internet, instead of limiting it.

VI. CONCLUSION

Congress has an important task in balancing the security risks that DPI presents with the innovative benefits of the technology. Online consumer protection is critical to the cyberhealth of U.S. citizens, but regulations that are imposed too quickly in response to perceived fears of what might happen will not be beneficial. The FTC's careful study of the concerns raised by behavioral advertising has provided a good framework for self-regulation. If, however, Congress does determine—as it has indicated it will—that self-regulation is not enough, then Congress must also take a calculated approach to online regulation. In doing so, congressional leaders should take time to look at both the benefits of, and concerns with, the technology. It should create a regulatory environment where ISPs that want to use DPI technology in safe ways are able to do so, and where new technologies that provide similar services are also able to thrive. By approaching DPI in this manner, consumers will likely have the opportunity to experience the benefits of the technology and have a safer, more personalized, and less expensive online experience. Congress should consider drafting regulations that (1) clarify how current legislation is intended to apply to DPI, (2) choose a consent regime that is both friendly to consumers trying to make decisions on behavioral advertisements and companies attempting to provide them, (3) review international approaches to the technology, (4) present a consistent policy for ISPs and Web site providers seeking to use behavioral advertising, and (5) consider the consequences to other DPI-based technologies that could be eliminated if overly stringent regulations are put in place.

The benefits that have resulted from the unregulated Internet are clear. The Internet has developed into what it is today because regulation has not interrupted its growth. Deployment has surged because revenue from multiple facets of the Internet have been allowed to grow, and people have recognized the value that the Web presents. In the interest of protecting sensitive information, the time has come for limited regulations to be put in place to protect consumers online; however, those regulations should not come at the expense of innovation. The reaction to a lack of regulation should not be heavy regulation. Congress should remember its tradition of focusing on the benefits of technology as it moves forward with behavioral advertisement regulations. If Congress gives consideration to both the positive and the negative aspects of the technology, it will likely draft moderate and responsible regulations that will best protect Americans while maintaining the best environment for Internet innovation.