Federal Communications Law Journal

Volume 64 | Issue 3 Article 6

5-2012

Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet

Joanna Penn
Indiana University Maurer School of Law

Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet

Joanna Penn*

I. INTRODUCTION 600
II. ONLINE BEHAVIORAL ADVERTISING 601
A. Targeting 602
B. Retargeting 603
C. What is FetchBack? 603
III. HOW USERS ARE TARGETED 604
A. The Type of Information Gathered 604
B. How that Information Is Gathered 604
IV. THE PROBLEMS WITH BEHAVIORAL TARGETING 605
A. Harm Through Profiling 605
B. Harm Through Data Fusion 606
C. Harm Through Information Leaks 607
D. Harm Through Lack of Consent 607
IV. PROPOSALS TO PROTECT INFORMATION PRIVACY 609
A. Legislation 609
B. FTC Regulations 610

* J.D. Candidate, Indiana University Maurer School of Law, May 2013; B.A. in Journalism, Indiana University, 2006. The Author would like to thank her citechecking team for their positivity, Matt Pfaff for his humorous negativity and supply of baked goods, and all members of the *Federal Communications Law Journal* for their revisions and dedication to perfection. She would also like to thank those that make law school and life in Bloomington not just bearable, but unbelievably enjoyable. Lastly, the Author would like to dedicate this piece to her mother, Elizabeth, a woman who does not have the Internet, but who will read this Note regarding the nuances of Internet with unwavering support and pride.

C. Privacy Policies and User Consent 612
1. Clearer Approval 612
2. Greater Transparency 613
D. User Consent 613
1. Opting-Out Option on a Retailer's Page 613
2. Opting-Out of FetchBack's Services 614
3. Opting-In 614
V. LOOKING FORWARD 615
A. Model for the Future 615
B. Conclusion 616

I. INTRODUCTION

You see a shadow lurking around the corner. You hear the creak of a door. You sense that someone is watching you. But then you look and listen, and you realize no one is there. But what if you were being watched, followed, and tracked and had no way of knowing? Enter behavioral advertising—the rich, talented, and mysterious Big Brother of the Internet.

Online shoppers feel bamboozled when they browse for a particular item online and then become "haunted" by the same, or sister, products. Julie Matlin contemplated buying a pair of shoes online at Zappos, but did not go through with the purchase.[1] Even though Matlin did not want the shoes, the shoes appeared to want Matlin: "An ad for those very shoes showed up on the blog TechCrunch. It popped up again on several other blogs and on Twitpic. It was as if Zappos had unleashed a persistent salesmen who wouldn't take no for an answer."[2] The ads that tirelessly trail users from site to site are a form of state-of-the-art online behavioral advertising known as retargeting—a type of advertising that "connects advertisers with past website visitors to entice those visitors to complete their online transactions or purchases."[3]

This Note will break behavioral advertising down in five parts. Part II explains the difference between targeting and retargeting and points out major companies in each category. Part III describes how online users are tracked. Part IV discusses the problems and concerns with tracking. Part V introduces ways in which law makers, the Federal Trade Commission

1. Miguel Helft & Tanzina Vega, *Retargeting Ads Follow Surfers to Other Sites*, N.Y. TIMES, Aug. 29, 2010, http://www.nytimes.com/2010/08/30/technology/30adstalk.html.

2. *Id.*

3. Catherine Schmierer, *Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 17 RICH. J.L. & TECH. 13 (2011), http://jolt.richmond.edu/v17i4/article13.pdf.

("FTC"), and individual online retailers can improve consumer education through transparency and obvious privacy and opt-out choices. Part VI provides a conclusion and a goal for the future of behavioral advertising.

II. ONLINE BEHAVIORAL ADVERTISING

Since the Internet boom of the mid-1990s, online advertising has evolved more than any other traditional form of advertising due, in part, to the advent of behavioral targeting.[4] Online behavioral advertising tracks consumers' online activities in order to deliver tailored advertising for goods and services that they are likely to click on, view, and ultimately purchase.[5] Cutting-edge algorithms analyze a user's online activity and deduce a user's likely inclinations.[6] Such a sophisticated method is made possible by the implementation of cookies, which are "small data file[s] (up to 4KB) created by a Web site you visit that [are] stored on your computer either temporarily for that session only or permanently on the hard disk (persistent cookie)."[7] The cookies are what enable data collectors to track and report the behavior of the user.

Using the data from the cookies, users are separated into profiles. These profiles provide information such as which websites and products have been viewed, demographics, and, when available, personality traits pertaining to the specific individual.[8] Tracking the user is extremely valuable because it allows businesses to narrow their approach and display items that more closely align with what interests a specific person, based on his or her predilections and search history.[9] Consumers have traditionally participated in offline, real-world tracking mechanisms—which record purchasing behavior and personal information—by signing up for customer loyalty programs and club cards in exchange for discounts or coupons.[10]

---

4. *Technology Overview*, GOOGLE, http://www.google.com/about/corporate/company/tech.html (last visited Apr. 10, 2012).

5. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter 2009 FTC STAFF REPORT].

6. *See* Tom Spring, *Algorithms That Rule the Web*, PC WORLD (Jul. 24, 2011, 9:00 PM), http://www.pcworld.com/article/236226-2/algorithms_that_rule_the_web.html.

7. *Definition of: Cookie*, PC MAGAZINE, http://www.pcmag.com/encyclopedia_term/0,2542,t=cookie&i=40334,00.asp (last visited Apr. 10, 2012).

8. Catherine Dwyer, *Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com*, 2009 AMS. CONFERENCE ON INFORMATION SYS. 2 (2009), *available at* http://aisel.aisnet.org/amcis2009/460/.

9. Andrea Stein Fuelleman, *Right of Publicity: Is Behavioral Marketing Violating the Right to Control Your Identity Online?*, 10 J. MARSHALL REV. INTELL. PROP. L. 811, 813–14 (2011).

10. Andrew J. McClurg, *A Thousand Words Are Worth A Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 66 (2003).

Contrary to tracking in the real world, online consumers are not signing up for behavioral targeting.[11] These shoppers are not making an active choice, but rather, they are merely silently "agreeing" to have information gathered concerning their habits and preferences while they load their cyber carts.[12] An example of such behavioral advertising is the following: an online shopper visits a clothing retailer and searches for blue sweaters. The potential consumer views blue sweaters but does not make a purchase. The shopper later visits Facebook and receives an ad for "blue sweaters on sale starting at $19.99." Interpreting what type of behavioral advertising this message is depends upon the previous actions of the user and the form of marketing a specific retailer employs for its needs.

A. Targeting

With a network of over eleven thousand web publishers and billions of advertisements placed online, DoubleClick is the leader when it comes to delivering targeted online advertising.[13] DoubleClick specializes in "collecting, compiling and analyzing information about Internet users through propriety technolog[y]" in order to provide the consumer the most appealing banner ads.[14] This task is completed by placing a cookie on a user's hard drive when they visit one of DoubleClick's client's sites—an action that is neither evident nor explicitly permitted by the user.[15]

DoubleClick's cookies collect submitted information in three forms: "GET" (information that is submitted as part of a website's address), "POST" (information that is submitted by fill-in multiple blank fields on a webpage), and "GIF" (information from tags that are put on affiliated websites).[16] Professor Joel Reidenberg states, "These cookies enable DoubleClick to track the clickstream of Internet users [sic] keyboard stroke by keyboard stroke across any of DoubleClick's 11,000 affiliated Web sites."[17] With the collection of the tracking data, profiles are then created. DoubleClick allegedly has more than one hundred million specific user profiles.[18]

---

11. *Id.*
12. *See id.*
13. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).
14. *Id.*
15. *Id.* at 503–04.
16. *Id.* at 504.
17. McClurg, *supra* note 10, at 82.
18. *DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 505.

B. Retargeting

The latest form of behavioral advertising acts as an intermediary between advertisers and consumers. Retargeting displays ads from websites that users have already visited in order to encourage them to purchase products or services in which they have shown interest.[19] "With retargeting you *only* target users that have visited your site and already had an experience with your brand."[20] Retargeting narrows the types of advertising images that are displayed, usually by showing products a user has already viewed, which increases the chances that the viewer has interest in the ad.[21] FetchBack is a leading company of such innovative marketing.

C. What is FetchBack?

FetchBack is the up-and-comer in advertising retargeting**.** With over 700 active advertisers under its belt and $400 million "fetched" sales for its clients, the company is becoming a household name among Internet retailers.[22] FetchBack's mission is simple: it wants to put messages in front of lost prospects who have left a website by reminding and urging them to come back and purchase the product they left behind.[23] But how does it get these customers back?

As FetchBack puts it, "[w]hen prospects leave [a company's] site and browse the Internet, [the site's] ads will display on other sites they visit, keeping [the original] website in their peripheral vision and top of mind."[24] FetchBack is also confident that these buyers will come back to the site and tend to make the purchase they had previously considered and will sometimes even add additional items to the cart.[25] But, the question still remains, how does FetchBack really do it?

---

19. Schmierer, *supra* note 3, at para. 2.

20. Joanna Lord, *Retargeting: What It Is & How to Use It*, SEOMOZ (Apr. 5, 2011), http://www.seomoz.org/blog/retargeting-basics-what-it-is-how-to-use-it.

21. *See id.*

22. *Why Should You Use FetchBack Retargeting?*, FETCHBACK, http://www.fetchback.com/whyfetchback.html (last visited Apr. 10, 2012).

23. *Id.*

24. *What Is Retargeting?*, FETCHBACK, http://www.fetchback.com/retargeting.html (last visited Apr. 10, 2012).

25. *Id.*

III. HOW USERS ARE TARGETED

A. The Type of Information Gathered

Personally identifiable information ("PII") is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[26] PII is not limited to a specific set of data but instead requires a case-by-case analysis to see if the information could be used to identify a specific individual.[27]

FetchBack claims that it only collects PII, such as names, email addresses, credit card numbers, and other distinguishable bits of data from those who have a FetchBack account and have registered the information.[28] Meanwhile, the majority of information collected is nonpersonally identifiable information ("non-PII") that is gathered from its partner sites.[29] Unlike PII, non-PII is simply anonymous data that, without more specific data added to it, cannot identify a specific person.[30] FetchBack also claims that none of the information it collects from partner sites can be used to identify a specific user.[31]

B. How that Information Is Gathered

An Internet user who is seen to be a prospective customer receives a cookie from FetchBack and FetchBack's partners when they visit FetchBack.com or, more commonly, one of the FetchBack advertiser websites.[32] FetchBack states that it has no control over what information its partners collect from cookies, but requires that it is only non-PII information for the purpose of serving retargeted ads.[33]

FetchBack also uses a "smart pixel" to track a prospect's activity.[34] Tracking with a pixel or a "web bug" is a process that involves placing tiny images, measuring only 1x1 pixel per inch, on webpages in order to track

---

26. Memorandum from Exec. Office of the President, Office of Mgmt. and Budget for the Heads of Exec. Dep'ts. and Agencies 8 (June 25, 2010), http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf [hereinafter Memorandum].

27. *Id.*

28. *Privacy Policy*, FETCHBACK, http://www.fetchback.com/privacy.html (last visited Apr. 10, 2012).

29. *Id.*

30. 2009 FTC STAFF REPORT, *supra* note 5, at 20 n.47.

31. *Privacy Policy*, *supra* note 28.

32. *Id.*

33. *Id.*

34. *Targeted Retargeting*, FETCHBACK, http://www.fetchback.com/targeting.html (last visited Apr. 10, 2012).

and record when someone views the page and additional information they leave behind.[35] FetchBack's pixel gathers intelligence about prospective buyers such as where they live, the sites and products they view, keywords they type, and, most importantly, what they have and have not purchased.[36] Yet, the real nuances of the company's pixel remain a secret. However, the company does reveal that "[t]his tiny pixel has one job: hunting and gathering. It passes no judgment."[37]

When an Internet user visits a website of one of FetchBack's advertiser clients, a pixel on that site places a cookie on the hard drive of the user.[38] Then, when that same user visits one of FetchBack's partner's websites, that site will identify the cookie on the hard drive, sending an alert that the user has visited a particular advertiser's website on an earlier occasion.[39] During this final step, an ad appears from that same advertiser (and FetchBack client) with either items similar or exactly the same as what the shopper previously viewed.[40] These clients are typically large retailers. FetchBack then records non-PII data including whether the user clicked on the ad, purchased an item, or simply ignored the image.[41]

IV. THE PROBLEMS WITH BEHAVIORAL TARGETING

The current issues that worry privacy advocates stem from the rate at which behavioral profiles are growing and how they are accumulating a myriad of personal information along the way.[42] Because the line between PII and non-PII becomes increasingly blurred as technology grows more sophisticated and tracking becomes more prominent, the risk of this consumer information being improperly gathered, stored, and disseminated becomes greater.[43] All the while, Internet users have few options to prevent tracking and to protect themselves.

A. Harm Through Profiling

Consumer profiling occurs in both the offline and online realms. However, it was not until recently that the mixture of the two mediums was

---

35. *See* Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET NEWS (July 12, 2000), http://news.cnet.com/2100-1017-243077.html.

36. *Targeted Retargeting*, *supra* note 34.

37. *Id.*

38. *Privacy Policy*, *supra* note 28.

39. *Id.*

40. *See id.*

41. *Id.*

42. *See generally* 2009 FTC STAFF REPORT, *supra* note 5.

43. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1865 (2011).

cause for concern. In 1999, the FTC began an investigation vis-à-vis behavioral profiling and the risks to consumers when DoubleClick (which specializes in online behavioral advertising) purchased Abacus Direct (which maintains a database of offline retail habits).[44] The FTC was concerned that the combination of the two sources of information would drastically change the way consumers could be profiled. The fear was that the merger of the companies could lead to non-PII becoming PII through a "super database" and the rights of consumers being violated.[45]

The FTC's fears were later found to be unsubstantiated because the investigations found that DoubleClick had not engaged in unfair trade practices.[46] More significantly, DoubleClick had not combined its online database with Abacus' offline database.[47] Even in the absence of a database merger, the business merger raised the possibility of such powerful profiling to occur in the near future. Even without the union of two of the leading behavioral advertising corporations, many concerns remain regarding the direction of extensive profiling.

B. Harm Through Data Fusion

Due to the emergence of new technology, such as smart phones, social media, interactive gaming systems, and other devices, non-PII has a greater potential than ever before to turn into PII. Non-PII can quickly become PII when additional information is made public or when other pieces of information are strung together.[48] Names, email addresses, and phone numbers found on social media sites can be linked with location tracked on a mobile device or data saved on retailer's sites, completing what was once an unsolvable puzzle. The FTC notes that "although industry has traditionally considered most IP addresses to be non-PII, it soon may be possible to link more IP addresses to specific individuals."[49]

Regardless of whether the information is identifiable or not, surveys suggest that Internet users are simultaneously surprised and concerned when they learn the truth behind online behavioral advertising practices.[50] Users assume their online activity is private, not profiled. A poll by the Consumers Union reports that over half of the users who were surveyed were "uncomfortable with [I]nternet companies using their browsing

---

44. *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 (S.D.N.Y. 2001).
45. *Id.*
46. *Id.* at 506.
47. *Id.*
48. Memorandum, *supra* note 26, at 8.
49. 2009 FTC STAFF REPORT, *supra* note 5, at 22.
50. *Id*. at 23–24.

histories to send relevant ads or third parties collecting information about their online behavior."[51]

C. Harm Through Information Leaks

Another concern with behavioral profiling is that sensitive information can fall into the wrong hands or be seen by the wrong eyes. This can be emotionally or financially harmful to consumers. With this merger of non-PII and PII, the risk of financial information being leaked, and financial accounts subsequently being hacked, increases considerably. Emotional damage can also occur when sensitive personal information is shared by multiple family members or individuals when there is only one computer in a household.[52] The FTC illustrates this issue with an example where one user searches topics regarding sensitive personal information and then the following individual (who uses the same computer) receives targeted ads associated with the previous user's search.[53] Such unintentional information sharing is due to retargeting, which is intended to be a helpful revenue-boosting tool by narrowly tailoring ads to a user's interests. When these advertisements appear with great frequency and specificity, however, the identity of the former user, along with his or her private information, can become public knowledge.[54]

D. Harm Through Lack of Consent

Even the lowest level of behavioral advertising can conceivably harm a consumer simply due to the user's lack of awareness that they are being tracked and of the resulting loss of privacy they incur.[55]

A proponent for greater user education feels that by "merely participating in the Internet economy, consumers lose control over which details about their private lives are known, and they have little control over who gets to learn of these details after the data passes into a profiler's hands."[56] Likewise, even when consumers have a degree of awareness that such tracking exists, it is often unclear what they are consenting to when reading a privacy policy or notice.

In the absence of federal legislation to enforce solid guidelines, the FTC uses privacy policies as a means of gauging and regulating

---

51. *Id.* at 24 n.52.

52. *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting,* 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 45 (2011).

53. 2009 FTC STAFF REPORT, *supra* note 5, at 23.

54. *See id.*

55. Berger, *supra* note 52, at 19.

56. *Id.* (footnotes omitted).

transparency in online profiling.[57] Online retailers are required to have privacy policies that include what information they will collect and what they intend to do with the information collected. The absence of such information may bring about FTC action.[58] The FTC deemed this form of transparency to be vital because a "[f]ailure to provide consumers with the means to make informed decisions constitutes an unfair trade practice," which is an area under the umbrella of the FTC's control.[59] By allowing a consumer to make an informed decision, the commercial organization, such as large online retailers, has given the individual the opportunity to consent to viewing the page, adding items to their cart, and making purchases.

The act of consent requires reasoned deliberate action. "Express consent is that directly given, either lira voice or in writing. Implied consent is that manifested by signs, actions, or facts . . . which raise a presumption that the consent has been given."[60] Consent is something that is implied in agreements.[61] But does active reasoning occur with privacy policies?

Using someone's name, likeness, or identity for commercial purposes, such as advertising, without consent is considered appropriation and is grounds for a tort claim.[62] The Second Restatement of Torts does not specifically state that an absence of consent is a necessary element of the tort "appropriation."[63] However, if there were clear and obvious consent, then there would be no cause of action. It can be inferred that this element is included in the tort, even though not overtly enumerated.[64] Yet, data-mining companies, third-party advertising corporations, social media giants, and online retailers appear to ignore the need for consent and do collect, analyze, sell, lease, and utilize a user's personal information—from their behavior and preferences to their values and lifestyles—all without affirmative consent from the user.[65] Even when there is notice, in the form

---

57. *See* FRED H. CATE, PRIVACY IN PERSPECTIVE 7 (2001); *see also* FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTIZING, MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 3 (Dec. 20, 2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

58. Brian Stallworth, Note, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, 62 FED. COMM. L.J. 465, 479–80 (2010).

59. *Id.* at 480; *see also* 15 U.S.C. § 45 (2006).

60. *Consent*, Black's Law Dictionary, http://blackslawdictionary.org/consent/ (last visited Apr. 10, 2012).

61. *Id.*

62. *Use of Name or Likeness*, U.S. LEGAL, http://privacy.uslegal.com/what-constitutes-a-violation/use-of-name-or-likeness/ (last visited Apr. 10, 2012).

63. *See* RESTATEMENT (SECOND) OF Torts § 652C (1977).

64. McClurg, *supra* note 10, at 128–29.

65. *Id.* at 129.

of a privacy policy or otherwise, the message is unclear and the only option is to click "ok," "yes," or "I agree" in order to move on. Yet, for a majority of users, there is no awareness that any of this action has taken place. Consequently, the question that remains is whether the court will deem this use of information, without being consented to, as worthy of tort protection without conclusive, demonstrable "harm" present.

IV. PROPOSALS TO PROTECT INFORMATION PRIVACY

One question that remains to be answered, and is of the utmost importance, is who should have control over the future of online privacy.[66] While some argue that the FTC is the most fitting agency to handle the issue, others believe that regulation must come from a legislative body that can mandate concrete laws. Prior to the devastation of the terrorist attacks of September 11, 2001, the subject of how to protect information privacy was one of the hottest topics in the United States.[67]

Before 9/11, there were approximately eighty bills that were in cue, waiting to be discussed and voted on, that focused on Internet privacy regulation and an additional five hundred that, to some extent, related to privacy.[68] However, public opinion changed after the attacks on 9/11, as did the opinions of legislators who represent their constituents.[69] With a perceived need to obtain vital information in trying times, the focus on privacy shifted from how to protect private information to how to access personal information.

A. Legislation

No statute covers the general collection of personal information online. "Unlike the European Union, which requires databases to be registered and approved by government data protection agencies, the United States has relied on the market and self-regulation to address privacy concerns."[70] Yet, many advocates for privacy are now pushing for concrete laws and rules regarding online privacy and protecting the rights of Internet users. The largest piece of legislation regarding information gathering, the USA PATRIOTAct, was passed by Congress in response to

66. *Id.* at 87.

67. *Id.* at 87–88.

68. Kelly Hearn, *Wild Web Hears Hoofbeats of Lawmakers*, CHRISTIAN SCIENCE MONITOR (Feb. 14, 2000), http://www.csmonitor.com/2000/0214/p20s1.html.

69. *See* McClurg, *supra* note 10, at 88–89.

70. *Consumer Privacy*, HARVARD UNIV., http://cyber.law.harvard.edu/ecommerce/privacy.html (last visited Apr. 10, 2012).

9/11.[71] This Act does not stand to protect private information, but rather to increase the power of the government when it comes to investigations, particularly those concerning online information.[72] Many privacy advocates are concerned about the amount of damage the Act will cause. EPIC.org states that perhaps the most troubling aspect is that, "[t]hough the Act made significant amendments to over 15 important statutes, it was introduced with great haste and passed with little debate . . . ."[73] Without intense debate, the Act lacks legislative history which is crucial to those in the judiciary when trying to interpret how to read and apply the Act accordingly.[74]

Privacy bills continue to be introduced, but as of yet, none have passed.[75] Aside from the rapid developments in technology and the difficulties with passing legislation that can both encapsulate the nuances of online privacy and remain current, an additional reason for this stand-still in legislation is that Congress may not be the best place for the guidelines to be created.[76]

B. FTC Regulations

Some privacy scholars believe the best place for power over privacy regulation is with the FTC. The FTC was formed out of Section 5 of the 1914 Federal Trade Commission Act.[77] This significant statute allowed the FTC to have "broad authority to regulate unfair and deceptive business practices."[78] The FTC has acquired power in many fields, such as the Internet, especially in those fields not overseen by other agencies.[79] The Act currently states that "unfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[80] The FTC's attention focused on online consumer privacy concerns following the advent of online commerce in the 1990s.[81] Retail

---

71. *USA PATRIOT Act*, EPIC.ORG, http://epic.org/privacy/terrorism/usapatriot/# introduction (last visited Apr. 10, 2012).

72. *Id.*

73. *Id.*

74. *Id.*

75. *See id.*

76. McClurg, *supra* note 10, at 91.

77. *Appendix 1 – Laws Enforced by the FTC*, FED. TRADE COMM'N, http://www.ftc.gov/opp/gpra/append1.shtm (last modified June 25, 2007).

78. *Id.*

79. *A Super-Power FTS Should Scare Advocates*, CBS NEWS (Apr. 14, 2010), http://www.cbsnews.com/stories/2010/04/14/opinion/main6394028.shtml.

80. *Appendix 1 – Laws Enforced by the FTC*, *supra* note 77.

81. 2009 FTC STAFF REPORT, *supra* note 5, at 4.

was moving from the inside of shopping malls to the inside of homes, but the need for consumer protection remained a key concern.

While there are no specific laws regarding online privacy, there are regulations. The FTC plays an integral role in shaping the best practices for the advertising industry. By the late 1990s, the practice of tracking consumer behavior online to more accurately personalize advertising had emerged as a focal point of FTC concern.[82] By the year 2000, controlling behavioral advertising became a priority of the FTC, but no direct measures were ever made, leading to the current self-regulation of the advertising industry.[83]

In 2009, the FTC issued a staff report on Self-Regulatory Principles for Online Behavioral Advertising ("Principles").[84] This report has proven to be fairly successful in setting the standards for the behavioral market. In fact, it has been noted that "several media organizations, including the Network Advertising Initiative ('NAI') as well as private companies follow the FTC's self-regulatory approach and have adopted similar principles."[85]

The 2009 FTC Principles focus on four governing concepts: (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 Using Sensitive Data for Behavioral Advertising.[86]

While the Principles are an innovative concept from the FTC and do provide guidance, some individuals believe they must be more rigid and explicit to produce meaningful results. Transparency and control are the first aspects addressed by the FTC and, yet, "the Principles do not specifically address when, where, and how disclosures and choice should apply."[87] Much like other agencies, the FTC must remain open to criticism and comments in order to clarify any ambiguous language and to shape the way e-commerce is conducted and consumers are protected.

---

82. *See generally id.* at i.

83. *See* Fuelleman, *supra* note 9, at 815.

84. *Id.* at 816.

85. *Id.*

86. 2009 FTC STAFF REPORT, *supra* note 5, at 46–47.

87. Fuelleman, *supra* note 9, at 816 (citing 2009 FTC STAFF REPORT, *supra* note 5, at 35).

C. Privacy Policies and User Consent

1. Clearer Approval

Due to the technology and Internet boom over the past decade, the FTC began working with several governing bodies and policymakers to determine the most effective method to write and display privacy policies. One issue with privacy policies is that most are not prominently displayed. Andrew McClurg states, "[The policy's] placement, length, and complexity appear calculated to ensure that consumers will not notice or read them. For example, Amazon.com's privacy policy link appears at the bottom of the long home page in what appears to be 4-point font."[88] The FTC has taken note of such complaints and has stated that it feels the best way for the information to be presented is in short statements. In the 2009 Report, commenters stated:

> [P]rivacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers. Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers . . . . [A] disclosure (*e.g.*, "why did I get this ad?") that is located in close proximity to an advertisement and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers. Indeed, such a disclosure is likely to be far more effective than a discussion (even a clear one) that is buried within a company's privacy policy.[89]

In addition to the text disclaimer which explains why the user was shown the ad, some businesses with an online presence have already begun to experiment with more creative ways, through more interesting designs and graphic treatments, to disclose this information.[90] The FTC encourages such work and adds that the creative treatment may be most effective if combined with consumer education programs.[91] These programs should explain not only what information is collected from consumers and how it is used, but also what tradeoffs are involved when users allow their information to be collected and shared.[92]

---

88. McClurg, *supra* note 10, at 130.

89. 2009 FTC STAFF REPORT, *supra* note 5, at 35–36 (footnotes omitted).

90. Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 19 (2009).

91. 2009 FTC STAFF REPORT, *supra* note 5, at 35–36.

92. *Id.* at 36.

2. Greater Transparency

Internet users, and especially online consumers, should have the right to know exactly what they are consenting to when they choose to visit a site, view a page, or make a purchase. But, time and again, they do not. Reviewing the language of the Zappos privacy policy, it is no surprise that Julie Matlin, the Zappos shopper,[93] was surprised when she saw the shoes she had previously viewed following her later on numerous websites.

Listed in the "Information Collection" section of the privacy policy, Zappos states, "[w]e may use third-party advertising companies to help tailor site content to users or to serve ads on our behalf."[94] And then those companies "may employ cookies . . . to measure advertising effectiveness . . . ." which is measured by data such as what pages users view, what products users are interested in, and which products, and how many of them, are finally purchased.[95]

Zappos provides other warnings with statements such as "we may share your information with affiliates under Zappos.com, Inc.'s control . . . . We may disclose such information in response to requests from law enforcement officials conducting investigations; subpoenas; a court order," and "[w]e may share non-personal information . . . with third parties such as advertising partners."[96] With such unclear language, how can a user actually weigh the risk of agreeing to a privacy policy? More so, once they have visited the site, how can they be sure that they are not still being tracked or that their information is not being shared? There is one clear solution: opt-out.

D. User Consent

1. Opting-Out Option on a Retailer's Page

Retailers and other online sites that offer consumers the opportunity to opt-out of data collecting, sharing, or profiling could argue that the failure to opt-out constitutes implied consent. To "opt-out" means that a user actively informs a company or website that she does not want her information collected or shared.[97] This action can occur at any time. While it seems to be a practical option to ensure privacy, opt-out is a mechanism

---

93. *See* Helft & Vega, *supra* note 1.

94. *Zappos.com's Privacy Policy*, ZAPPOS, http://www.zappos.com/privacy-policy (last visited Apr. 10, 2012).

95. *Id.*

96. *Id.*

97. *Opt-Out*, NETLINGO, http://www.netlingo.com/word/opt-out.php (last visited Apr. 10, 2012).

that "places the burden on consumers to inform companies that they do not want their data shared."[98] Absent express communication of this desire, companies may freely collect, profile, and share an individual's personal information.

2. Opting-Out of FetchBack's Services

Users may opt-out of FetchBack, delete the cookies from a browser, or even have a browser notify them when a cookie is set.[99] By opting-out or deleting cookies, FetchBack is no longer able to operate. A user can also opt-out by visiting the Network Advertising Initiative website.[100] However, using this method, FetchBack must maintain a cookie on the user's browser in order to recognize the user as someone who has opted-out. Additionally, each time an individual uses a different computer or a different browser, they must opt-out again.[101] Even more time-consuming, yet empowering for consumers is an opt-in system.

3. Opting-In

While companies are finally making strides by having opt-out choices more prominent on their sites, some organizations are urging Congress and the FTC to demand an "opt-in" choice regarding commercial use of information. Opting-in requires an active choice to share information.[102] Therefore, commercial entities would actually have to stop and receive permission from users before they could begin sharing, or even collecting, data.[103]

This type of consent is being encouraged from those in the tech industry. During a Senate Committee hearing entitled "Privacy Implications of Online Advertising," representatives from Verizon, AT&T, and Time Warner Cable strongly voiced that their industry should be self-regulated when it comes to online behavioral advertising. But, in order to do this, they called for "a requirement that companies obtain opt-in consent from consumers before collecting online information for behavioral advertising purposes."[104]

---

98. McClurg, *supra* note 10, at 133.

99. *Privacy Policy*, FETCHBACK, http://www.fetchback.com/privacy.html (last visited Apr. 10, 2012).

100. *Id.*

101. *Id.*

102. Michael Duffy, *Opt-In Consent for Online Behavioral Advertising: A Fair Bargain for Consumer Privacy*, PETERSWIRE.NET 2–3, http://www.peterswire.net/finalbehavioral papers/duffy-final.pdf.

103. *See* McClurg, *supra* note 10, at 133.

104. 2009 FTC STAFF REPORT, *supra* note 5, at 16.

Moreover, if the commercial entity decides to use the consumer's information in a way that is inconsistent with the notice the user has already agreed to, then the business must update the notice accordingly and obtain the opt-in consent of the consumer again before using the information.[105] While opting-in may bring consumers directly into the market, give them a sense of empowerment, and minimize their risks to their privacy, will consumers choose to read through lengthy privacy statements? More importantly, will users actually know what they are consenting to or just sign on the dotted line, per usual?

V. LOOKING FORWARD

A. Model for the Future

The issue of online privacy and misuse of consumer's personal and nonpersonal information has not been forgotten. Though not as much of a hot-button issue as it once was, House Bill 5777, introduced on July 18, 2010, demonstrates that Congress still considers it an issue worth reviewing.[106] While the bill did not move forward, its standards for those who collect and store data are innovative, clear, and a model for the future.

The Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act ("BEST PRACTICES Act") serves to "foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information . . . ."[107] The BEST PRACTICES Act requires a covered entity (one who is engaged in commerce and collects or stores data containing covered or sensitive information) to make the following information available to individuals whose information it collects: (1) the identity of the collector; (2) a description of what the entity is collecting, why they are collecting it, and how it will be potentially used; and (3) a report of how the information is collected and how the collector will limit its collection, use, and disclosure.[108]

Furthermore, the proposed bill prohibits a commercial entity from: (1) collecting, using, or disclosing an individual's information unless it provides the data in clear and easy-to-understand notices that adhere to FTC regulations; (2) collecting or using an individual's information unless they have given consent or at least have been notified; and (3) disclosing

105. Duffy, *supra* note 102, at 3.
106. *See* BEST PRACTICES Act, H.R. 5777, 111th Cong. (2010).
107. *Id.*
108. *Id.*

information about an individual to a third party (targeting or retargeting company) unless the individual has already given affirmative consent.[109]

B. Conclusion

Although retargeting companies appear to collect and utilize less data from cookies than the large targeting corporations, such as DoubleClick, the end result of retargeting can be more perplexing for the consumer because the advertisements being displayed time and again are more obviously meant for them, and yet, consumers are unaware they are being tracked, how they are being tracked, and the mechanics behind such advertising. The constant barrage of previously-viewed images may become ineffective over time or it may encourage users to not shop where they are followed.

Requiring all users to opt-in to online tracking or to explicitly agree to the privacy policy of every website they visit is too restricting, time-consuming, and unrealistic—for both the user and the site. However, by the FTC setting out guidelines regarding how commercial entities should present their privacy policies and tracking operations, the user becomes educated and informed. A push from both Congress with bills such as Best Practices Act, which implements harsher standards for entities who collect and store data, and the FTC, with clear and reasonable guidelines regarding privacy policies and consent, behavioral marketing will have the potential to become a respected and well-understood industry.

FetchBack is not the issue. Third party advertisers are not to blame. While they serve as the middle man, you should not shoot the messenger. Transparency and trust must come from the retailers we trust and depend on to deliver our goods, not to deliver our personal data. Zappos, are you listening?

---

109. *Id.*