DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 22
Issue 1 *Fall 2011*

Article 7

Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online

Stephanie A. Kuhlmann

DO NOT TRACK ME ONLINE:

THE LOGISTICAL STRUGGLES OVER THE RIGHT "TO BE LET ALONE" ONLINE

> "The Internet is 'the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.'"– Eric Schmidt [1]

I. INTRODUCTION

If a stranger approached you on the street, would you divulge your name, address, email, and account passwords? Hopefully you would not. But, this is essentially the exchange you make, perhaps unknowingly or unwillingly, when you use the Internet.

The Internet has become a global platform for commerce, socializing, and communication.[2] As such, technology is essential to economic growth, and the Internet plays a critical role in the American economy and its prosperity.[3] In addition to affecting our economy, the Internet is transforming our notions of privacy. The Internet is rich in information, including information about Internet users. Protecting privacy involves protecting users' personal information to ensure that they have the confidence and ability to take advantage of the Internet's benefits.[4] Privacy breaches cause

---

1. Staff Writer, *Net Founders Face Java Future*, CNET NEWS.COM (Apr. 2, 1997, 5:30 PM), http://news.cnet.com/Net-founders-face-Java-future/2100-1001_3-278526.html. This quote was printed in an article by CNET News, as Eric Schmidt transitioned from chief technology officer of Sun Microsystems, to chairman of Novell. *Id.* In 2001, Schmidt became CEO of Google Inc. *Management Team*, GOOGLE.COM, http://www.google.com/about/corporate/company/execs.html#eric (last visited Aug. 29, 2011).

2. *Issues: Technology*, WHITE HOUSE http://www.whitehouse.gov/issues/technology (last visited Sept. 25, 2011).

3. *Id.*

4. *Prepared Statement of the Federal Trade Commission on Privacy and Data Security: Protecting Consumers in the Modern World Before the H. Subcomm. on Commerce, Mfg., and Trade, H. Subcomm. on Commc'ns &*

a variety of harms, including the exposure of sensitive, personal information to unintended sources, and financial losses.[5] Furthermore, protecting privacy is essential to fostering a competitive Internet economy.[6] Privacy laws directly affect electronic commerce (e-commerce) by dictating the practices of online companies with respect to the collection and use of personally identifying information, which in turn, affects consumer confidence.[7]

Despite the value American culture places on privacy, privacy protection is incomplete in regard to information privacy. As federal lawmakers compete for comprehensive privacy policies,[8] this Article examines two bills targeting online privacy issues related to tracking users online: the Do-Not-Track Online Act of 2011, Senate Bill 913[9]; and the Do Not Track Me Online Act of

---

Tech., H. Comm. on Energy & Commerce, 112th Cong. *1 (F.T.C. 2011) [hereinafter Brill] (statement of Julie Brill, Comm'n of the F.T.C), *available at* 2011 WL 2614552.

5. *The Views of the FTC, the FCC, and NTIA, Hearing on Internet Privacy Before the H. Subcomm. on Commerce, Mfg., and Trade, H. Subcomm. on Commc'ns & Tech., H. Comm. on Energy & Commerce*, 112th Cong. (2011) [hereinafter Strickling] (statement of Lawrence E. Strickling, Assistant Sec'y for Comm'ns & Info., Nat'l Telecomm. & Info. Admin., U.S. Dep't of Commerce), *available at* http://ntia.doc.gov/category/privacy.

6. Cameron Kerry & Christopher Schroeder, *White House Council Launches interagency Subcommittee on Privacy & Internet Privacy*, WHITE HOUSE BLOG (Oct. 24, 2010, 10:10 AM), http://www.whitehouse.gov/blog.

7. 2 IAN C. BALLON, E-COMMERCE AND INTERNET LAW § 26.01 (2011). The author also discusses two additional ways in which privacy laws affect the conduct of E-commerce: 1) laws governing privacy can affect employee rights with respect to email and Internet usage at a company's intranet or Internet; and 2) publicity rights, based on privacy laws, potentially crucial in licensing website content. *Id.* These other two areas are beyond the scope of this Article. The term "personal information" used in this Article is consistent with Ballon's definition, of information that both identifies and potentially identifies a person. *Id.* at n.7.

8. *See* Commercial Privacy Bills of Rights Act of 2011, S. 799, 112th Cong. (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011); Personal Data Privacy and Security Act of 2011, S. 1151 112th Cong. (2011).

9. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011).

2011, House Bill 654.[10] The "Do Not Track" (DNT) Bills seek to restrict the online tracking of user information by requiring that Internet companies abide by a user's preference to opt out of data collection.[11] The legislation is aimed at companies that collect and analyze data, but the Bills provide exceptions, allowing companies to engage in currently accepted business practices.[12] Furthermore, state, local, and federal governments are exempt from obeying the opt-out setting.[13] If enacted, the Bills will grant both the Federal Trade Commission (FTC) and the states' attorneys general authority to enforce compliance with users' online privacy preferences and levy civil penalties.[14]

Although the proposed DNT Bills aspire to provide online privacy protection, they are ineffective solutions for insulating users from the harm of online surveillance because of their overly broad scopes and unavoidable, negative consequences. Vague terminology leaves users vulnerable to behavioral tracking on social networking websites, while targeting some harmless first party uses of data. Also, the enforcement power of the proposed legislation is diminished by the lack of a private right of action for users to remedy their breaches of harm. An inflexible DNT mechanism will strip away free Internet content and customization.

Part II of this Article will present background materials. A historical overview of the concept of Privacy as it applies to information technology, rather than personal autonomy rights, will supply the necessary framework for the overall discussion, while a discussion of the modern technological concerns will provide the essential context. Part II will also review the online industry's self-regulation practices and the FTC's enforcement capabilities currently in place. Part III will present a brief synopsis of the proposed Bills and the statutory provisions. Finally, Part IV will present an analysis of the possible effects of the Bills, both

10. Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. (2011).

11. *See* H.R. 654 § 3(a); S. 913§ 2(a).

12. For general exemptions, *see* H.R. 654 § 3(d)(1)-(7); S. 913 § 2(b).

13. H.R. 654 § 2(2)(A); S. 913 § 2(a) (limiting the Bill in application to individual providers of online services and mobile applications).

14. For general enforcement provisions, *see* H.R. 654 § 3; S. 913 § 3.

intended and unintended, as the Bills place mandates on online businesses and user interactions.

II. BACKGROUND

This section will provide a brief historical overview of the concept of Privacy, followed by an overview of current technology, cyber-security, e-commerce and Internet law.

A. Traditional Privacy Concepts

The United States Constitution provides many protections of privacy rights from governmental intrusion, such as the protection of thought, religion, private speech, and the home.[15] In *Griswold v. Connecticut*, Justice Douglas noted that the "right of privacy . . . is a legitimate one."[16] In conjunction with the Constitutional guarantees, codified and common law privacy rights also exist.[17]

In 1888, Judge Thomas M. Cooley first defined the legal concept of privacy as the right "to be let alone."[18] Shortly thereafter, Samuel D. Warren and Louis D. Brandeis declared the concept of a common law right to privacy in their seminal article, *The Right to Privacy*.[19] The authors reiterated that privacy was one of the rights most prized by society and threatened by the "evil" invasion of technological advancements, such as photography and newspapers, which permitted the media to bring previously private details into the public sphere.[20] Concern over preserving the private sphere and domestic life led to their conclusion that the law "must protect privacy on the principle of an 'inviolate personality.'"[21] They championed for a recognized right to

15. *See generally* U.S. CONST. amends. I-IV.

16. Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965).

17. *Id.* *See also* RESTATEMENT (SECOND) OF TORTS § 652A (1977) (outlining William Prosser's enumerated torts).

18. J. THOMAS MCCARTHY, RIGHTS OF PUBLICITY AND PRIVACY § 1.9 (2d ed. 2011) (citing THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888)).

19. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-96 (1890).

20. *Id.* at 193-95.

21. *Id.* at 205.

privacy, defining that right as the "right to be let alone."[22] Thus, Warren and Brandeis laid the foundation for the concept of privacy as control over information about oneself. Presently, advanced technologies provide a new rationale for the authors' concerns, as Internet and software innovations facilitate the online collection and dissemination of users' information.

In his formative article, Professor William Prosser distinguished four separate torts for the invasion of privacy: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of another's name or likeness; (3) unreasonable public disclosure of private facts; and (4) publicity that unreasonably places the other in a false light before the public.[23] Although each tort is designed to protect a different facet of privacy, they are linked through the commonality of the right of the plaintiff "to be let alone."[24]

Most states recognize at least one of Prosser's common law invasions of privacy torts.[25] Yet, many courts hold that privacy rights do not exist in voluntarily disclosed information unless the relationship is fiduciary in nature, or maintains confidential characteristics, such as medical information.[26] Furthermore, many courts evaluate the issue of privacy on the basis of an expectation of privacy, and whether this expectation is enforceable in law.[27] For example, if an individual posted an opinion on an Internet

22. *Id.* at 193.

23. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

24. *Id.*

25. *See generally The Privacy Torts: How U.S. State Law Quietly Leads the Way In Privacy Protection*, PRIVACILLA.ORG (July 2002), http://www.privacilla.org/releases/Torts_Report.html. The appendix lists key cases, statutes, and resources by state. *Id.*

26. *See* Zieve v. Hairston, 598 S.E.2d 25, 30 (Ga. Ct. App. 2004) (holding that hair transplants were private facts and that the plaintiff did not waive his right to keep his treatment secret by consenting to advertising limited to the defendant's place of business and television stations within 500 miles).

27. *See* United States v. Stults, 575 F.3d 834, 842-43 (8th Cir. 2009), *cert. denied*, 130 S. Ct. 1309 (2010) (holding that the defendant's privacy was not invaded, because he lacked a reasonable expectation of privacy for his downloaded computer files containing child pornography. The court reasoned that his files were accessible to others for file sharing, based on his installation and use of file sharing software).

blog, and signed their name, that individual could not have a reasonable expectation to privacy.[28]

An exception to the general lack of enforcement of informational privacy rights occurs when the Federal Trade Commission (FTC) penalizes companies for not adhering to their own publicized privacy policies. For instance, Toysmart, an online retailer majority-owned by Walt Disney Company, ceased operations in May 2000, and solicited bids for its assets, including customer lists and profiles of children.[29] Toysmart's privacy guidelines had been certified by TRUSTe, a company that gives its seal of approval to websites that meet its criteria for safeguarding customer privacy.[30] In *Federal Trade Commission v. Toysmart.com, LLC*, Toysmart was held liable for the sale of personal customer information to third parties, contrary to the express terms of its privacy policy stating that personal

---

28. *See also* Indep. Newspapers, Inc., v. Brodie, 966 A.2d 432, 440 (Md. 2009) (holding that the Circuit court judge abused his discretion when ordering the identification of five anonymous Internet discussion forum participants.) In *Brodie*, the court explained:

> the decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry.

Id.

29. Associated Press, *Privacy at Issue as FTC Sues Toysmart.com*, L.A. TIMES (July 11, 2000), http://articles.latimes.com/2000/jul/11/business/fi-51030.

30. *Id.* TRUSTe brought Toysmart's actions to the FTC's attention. *Id. See generally About TRUSTe*, TRUSTE, http://www.truste.com/about_TRUSTe/index.html (last visited Sept. 20, 2011). Since 1997, TRUSTe has marketed itself as the leading online privacy solutions provider, offering their consulting services to ensure their clients' compliance with evolving privacy requirements. *Id.* Based upon ideals of transparency, choice and accountability regarding the collection and use of personal information, TRUSTe promotes the use of its privacy seal as a symbol of responsible privacy practices. *Id.*

information would not be disclosed to third parties.[31] Toysmart was required to delete and destroy all customer information in their possession, pursuant to the Children's Online Privacy Protection Act of 1998 (COPPA).[32] An Internet unit of the Walt Disney Company paid Toysmart $50,000, for the toy company to destroy its records.[33]

B. Digital Footprints and Their Uses

When it comes to the Internet, the ability to be left alone is problematic. Whether a user is browsing online, perusing a social networking site, or shopping in an online store, a user's preferences, activities, and interests are recorded and classified by a variety of technological tools, such as the "cookie."

A "cookie" is a program placed on a user's hard drive, commonly as a text file, and identifies the particular user by browser program and version.[34] A cookie is used by a website operator to send state information to a user's browser, and for the browser to return the state information to the origin website.[35] The state information can be used for many purposes including: authentication, identification of a user's session, user preferences, shopping cart contents, or anything else that can be facilitated through storing text data.[36] Cookies can also collect login information, including usernames, search terms, and passwords.[37]

---

31. FTC v. Toysmart.com, LLC, No. 00-11341-RGS, 2000 WL 34016434, *1-*2 (D. Mass. July 21, 2000).

32. *Id.* at *2 (citing 15 U.S.C. §§ 6501 *et seq.*). Pursuant to the Children's Online Privacy Protection Act of 1998 (COPPA), and its implementing regulations, defendants were required to delete and destroy all information collected in violation of 16 C.F.R. § 312 within ten days of the Order. *Id.*

33. Associated Press, *Toysmart to Destroy Data, Be Paid*, L.A. TIMES (Jan. 10, 2001), http://articles.latimes.com/2001/jan/10/business/fi-10470.

34. 67 AM. JUR. 3D *Proof of Facts* § 1 (2011).

35. A. Barth, *HTTP State Management Mechanism*, INTERNET ENGINEERING TASK FORCE (IETF), UNIV. OF CAL. BERKELEY 6 (Apr. 2011), *available at* http://tools.ietf.org/pdf/rfc6265.pdf. A "cookie" can also be referred to as an HTTP cookie, web cookie, or browser cookie. *Id.* at 4.

36. *Id.*

37. Catherine Schmierer, *Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the*

Disabling cookies can involve many steps and require a moderate level of technical knowledge. Since cookies are browser-specific, disabling all cookies for a computer entails disabling the cookies for each browser program used on that computer.[38] Moreover, a basic cookie contains a unique identification number that identifies the particular computer it is filed on.[39] If more than one person uses a computer, the cookie will store information related to all users.[40] Most users are unaware that cookies are placed on their computers because they are designed to be invisible.[41] Furthermore, cookies are commonly encrypted, so even if a user found the cookie program and opened it, the data would be unreadable.[42] Consequently, a user cannot easily learn that his or her online activities are tracked.

Behaviorally targeted advertising is online advertising tailored to a user's personal interests, indicated by the user's online activity.[43] This type of advertising uses cookies to compile and gather user-data across multiple websites.[44] Thus, unlike traditional window-shopping, a user's Internet browsing experience can be captured and analyzed, and online merchants can collect the styles, colors, or dollar amounts of the goods website visitors peruse, and use that information to enhance their

---

Need for Regulation, 17 RICH. J.L. & TECH. 13, 10 (2011), *available at* http://jolt.richmond.edu/v17i4/article13.pdf.

38. *Proof of Facts, supra* note 34.

39. *Id.*

40. *Id.*

41. Schmierer, *supra* note 37, at 10.

42. *Id.*

43. *Id.* at 8.

44. *Id.* at 10. Cookies can be divided into two categories: browser-based and Flash cookies. *Id.* Browser-based cookies are easily removed by deleting the online browsing history in each Internet browser program. *Id.* Flash cookies are more insidious, because they are able to recreate deleted browser cookies. *Id.* at 10-11. Other common techniques of gathering user data involve the use of Spyware and Adware. *Id.* at 11. Spyware is software that is downloaded onto a user's hard drive, and collects and transmits that user's information. *Id.* at 12. Adware similarly transmits a user's data, but is not installed on a user's hard drive and instead lives on the Internet. *Id.* Adware tracks a user's online activity and can cause pop-up advertisements on the user's screen when the user views particular sites. *See id.*

business by redesigning their website for ease of shopping, or selecting inventory based on popularity.[45] The ease of information collection distinguishes the online venue from traditional means of commerce, raising new consumer concerns about information gathering.[46]

Behavioral advertising is one aspect of a growing industry which has subverted the original, benign purpose of the cookie, which was to ease the use of a user's frequently visited websites.[47] The sale of aggregated data collections has spawned a new industry, illustrating how "consumer privacy is under siege."[48] For instance, Acxiom Corporation, one of many information data-gathering companies, maintains a database about consumers' lifestyles, hobbies, ages, home ownerships, and provides this information to marketers.[49] In 2009, Acxiom's database maintained 10 billion records monthly, and 3 billion consumers were added daily.[50] By August 2011, Acxiom increased its database to include over 20 billion customer profiles and browser records, and it integrates over 4 billion customer records each day.[51] Collections of user data, like those provided by Acxiom, are important to marketers because they provide "'a deeper understanding of [its] customers and prospects,'"[52] and can potentially increase the "click-through rate."[53] Through this

45. BALLON, *supra* note 7.

46. *Id.* (citing PRIVACY ONLINE: A REPORT TO CONGRESS 40 (FTC June 1998)).

47. *Proof of Facts, supra* note 34, § 4.

48. Pamela Jones Harbour, Comm'r, Fed. Trade Comm'm, Remarks Before FTC Exploring Privacy Roundtable 2 (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

49. Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant*, 45 IDAHO L. REV. 317, 328 (2009).

50. *Id.* (citing *Acxiom Overview*, ACXIOM, http://www.acxiom.com/overview (last visited Feb. 28, 2009)).

51. *About Us*, ACXIOM, http://www.acxiom.com/ABOUT_US/Pages/AboutAcxiom.aspx (last visited Oct. 28, 2011).

52. Kane & Delange, *supra* note 49, at 328-39.

53. Stacey L. Dogan, *Trademark Remedies and Online Intermediaries*, 14 LEWIS & CLARK L. REV. 467, 478 (2010). The "click-through rate" indicates the number of times a user is diverted from the desired website, on which the advertisement is placed, to the advertiser's website. *Id.* The rate is found by

technique of aggregating and evaluating informational data, called data mining, the Air Force developed technology to detect insider threats.[54] Air Force researchers built a graph from a large body of collected data from emails, and identified individuals who appeared alienated or possessed a "hidden agenda."[55] Many companies and institutions are in the business of "trafficking" network data, and such information can reveal intimate details of a person's life.[56] In the Internet Age, data is currency and the larger the data set, the larger the potential profit.[57] For instance, it is projected that by 2016, spending on online advertising will almost double to $44 billion, from $26 billion in 2010.[58] Furthermore, by 2016, mobile advertising revenue is expected to grow to $1.8 billion, and online video advertising could triple, to $3.7 billion.[59]

On average, consumers do not expressly consent to the collection of their personal information, because they are either unaware data collection is occurring or do not understand the potential consequences.[60] For instance, website designers typically place their privacy policies and terms of use on the home landing page. Within the policy, a website details the information on their use of cookies and placing them on the user's computer.[61] Yet, the disclosures are often difficult to comprehend and do not offer

---

dividing the total number of clicks an advertisement receives by the number of time the advertisement is displayed. *Id.*

54. Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14 FIRST MONDAY 10 (Oct. 5, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. The authors' study is discussed in the following section. *See infra* notes 112-14.

55. *Id.*

56. *Id.*

57. Harbour, *supra* note 48, at 2.

58. Sara Forden, *Online Privacy: Can the U.S. Get Its Act Together?*, BLOOMBERG BUSINESSWEEK (May 12, 2011, 5:00 PM), http://www.businessweek.com/magazine/content/11_21/b4229027916671.htm. Projections were forecasted by Alex Feldman, manager of global forecasting at MagnaGlobal, a media researcher. *Id.*

59. *Id.*

60. Harbour, *supra* note 48, at 2-3.

61. *See, e.g.*, *id.* at 3-4.

practical alternatives for opting out, other than not using the website at all.[62]

C. Crossing the Digital Line

Users need an Internet that is safe and secure.[63] Data security entails employing security measures to ensure "availability, access, confidentiality, integrity, and authenticity," of collected consumer data.[64] While there cannot be absolute security, companies can utilize technical, physical, and administrative measures to ensure the maximum amount of security possible for their businesses.[65] For instance, technical security measures include implementing hardware or software to control access to information on computers.[66] Physical security measures protect computers from tangible threats, such as natural disasters.[67] Administrative security measures include protecting a network of data through personnel controls.[68] Without sufficient data security controls, there cannot be effective data privacy.[69]

Historically, data privacy concerns focused on protecting personally identifiable information (PII), defined as:

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, data and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as

62. *Id.* at 2-3.
63. *Issues: Technology*, WHITE HOUSE, *supra* note 2.
64. Kevin Cronin, *Best Practices and the State of Information Security*, 84 CHI.-KENT L. REV. 811, 812, 814 (2010).
65. *Id.* at 812.
66. *Id.* at 813.
67. *Id.*
68. *Id.*
69. Strickling, *supra* note 5.

> medical, educational, financial and employment information.[70]

Other data information, like cookie data or IP addresses, were useful to online companies, but could not identify an individual user, or anything particular about him, except that he viewed a particular website.[71] In light of new technologies and data aggregation techniques, the distinction between identifying information and non-identifying information has been blurred by the aggregation of anonymous details about an Internet user with identifying information from other sources.[72] For instance, a user may be identified by non-PII data if that information is combined with other information obtained from Internet Service Providers (ISP).[73] This is a real concern, because information about users is often traded between websites and ISPs.[74] Contracts can be formed between ISPs and marketers to exchange information collected from website use, such as a user's Internet Protocol (IP) address.[75] The website operator sends an advertisement addressed to the user of a certain IP address, and the ISP can pass it along to the individual account holder.[76]

---

70. Erika McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* 2-1 (Nat'l Inst. of Standards and Tech., Special Publication 800-122 (2010)) [hereinafter *Guide to PII*], *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. This article employs a working definition of PII as developed by the Government Accountability Office (GAO). *Id.* For the GAO's definition and explanation, *see* Gov't Accountability Office (GAO) Report 08-343, *Protecting Personally Identifiable Information*, (2008), *available at* http://www.gao.gov/new.items/d08343.pdf.

71. BALLON, *supra* note 7.

72. *Id.*

73. *Proof of Facts, supra* note 34, § 2.

74. *Id.* § 2.

75. *Id.*

76. *Id.* This system can be automated so the transmittal is instantaneous when a user clicks on an advertisement. *See* United States v. Forrester, 495 F.3d 1041, 1048 (9th Cir. 2007), where the court found that use of computer surveillance techniques that revealed the addresses of email messages and visited websites, and the total amount of data transmitted to or from the user's Internet account, did not constitute a "search" within the meaning of the Fourth

The aggregation of potentially identifying data could produce harmful, unintended consequences.[77] Harm, meaning adverse effects experienced by the user, includes negative or unwanted effects that can be socially, physically, or financially damaging.[78] Harm to individuals from privacy breaches includes the potential for identity theft, financial loss, physical harm, blackmail, discrimination, and emotional or mental distress from embarrassment.[79]

1. Breach of Privacy: Financial Harm

Financial harm,[80] including identity theft and financial fraud, is one type of harm occurring from breaches of data privacy. One method of disclosure involves companies' inability to properly secure their data.[81] For instance, through negligence, companies

---

Amendment. The court reasoned that Internet users have no expectation of privacy for the addresses of their email messages or visited websites because users should know that that information is sent to third parties, such as their ISP. *Id.* at 1049. Moreover, the addresses did not contain the content of the emails. *Id.*

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

78. *Guide to PII*, *supra* note 70, at 3-1.

79. *Id.*

80. Consumers' informational data has varying worth to identity thieves, ranging from $.90 for a Social Security number, to $1,000 for a bank account number. Kevin P. Kalinich, *Red Flags, Broken Hearts, & Data Breach Stimulus: Insurance for Breaches of Data Privacy and Information Security*, AON, 4 (June 2009), http://one.aon.com/files/red_flags_broken_hearts.pdf. Victims of identity theft can spend an average of 25 - 175 hours trying to repair the harm. *Id.* One survey report found that 8.1 million adults in the United States were identity fraud victims in 2010, and the average out-of-pocket cost due to identity fraud was about $631 per incident, including the expenses of paying off fraudulent debt and legal fees. Jennifer Saranow Schultz, *The Rising Cost of Identity Theft for Consumers*, N.Y. TIMES (Feb. 9, 2011, 12:01 PM), http://bucks.blogs.nytimes.com/2011/02/09/the-rising-cost-of-identity-theft-for-consumers/. This figure increased 63% since 2009. *Id.*

81. Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 21 (2011).

may lose or misplace backup tapes, laptops, smartphones, or other forms of portable data storage containing sensitive user data.[82] Or, customer data can be stolen, as opposed to lost, as in the case of the TJX data breach.[83] According to the FTC Complaint, TJX, with over 2,500 stores worldwide, failed to use reasonable and appropriate security measures to prevent unauthorized access to customer information on its computer networks.[84] Network intruders exploited TJX's security gaps, and collected tens of millions of payment card numbers, as well as personal information of about 455,000 customers.[85] Many consumers needed to obtain new drivers' licenses or identification cards because some of the stolen personal information included Social Security numbers.[86] The FTC explained that this information was particularly sensitive because it could facilitate payment card fraud and other harm, making it an unfair act or practice.[87] The settlement with TJX required the company to establish and maintain a comprehensive security program, reasonably designed to protect the integrity of their customer's personal information.[88] The TJX data breach occurred over a period of years, and demonstrates how a data breach can be an extremely expensive, operational risk for companies, as well as a privacy concern for consumers.

Companies' security can be intentionally breached by computer hackers or malware programs.[89] For example, in mid-April 2011, hackers breached a known security vulnerability of Sony

82. *Id.*

83. *See* In re TJX Co.s, No. C-4227, 2008 WL 3150421, *2 (F.T.C. July 29, 2008).

84. *Id.* at *1-2.

85. *Id.* at *2. Specifically, the agency charged that TJX: (1) created an unnecessary risk to personal information by storing it and transmitting it in clear text; (2) did not use readily available security measures to limit wireless access to its networks; (3) did not require employees to use strong or different passwords; (4) failed to use readily available security measures to limit access among its computers and the Internet; and (5) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations. *Id.*

86. *Id.*

87. *Id.* at *1, *3.

88. *Id.* at *4.

89. Berger, *supra* note 81, at 21.

Corporation, the maker of the PlayStation 3 videogame console, and gained access to Sony's data files on their customers.[90] The hackers stole the names, birthdates, mother's maiden names, passwords, and more, for over 100 million customers.[91] Sony said that the stolen credit-card numbers were encrypted, which would make the codes difficult to read, and there was no evidence that the main credit card database was comprised.[92] However, the stolen data included debit card numbers and expiration dates.[93] This data breach resulted in a privacy breach for Sony's customers, and "may have exposed customers to years of potential identity theft."[94] Estimates of Sony's financial impact from the data breaches have soared beyond $171 million, due to credit-card fraud, repairs to network security, and marketing campaigns.[95] When sensitive financial data is distributed to unintended sources, users can easily suffer financial harm. Data security is a key requirement for maintaining consumer privacy, and in turn, consumer trust in the online marketplace. Consumer trust is critical to the Internet thriving as a center for economic, political, and social development.[96]

Privacy breaches can also result from companies intentionally dispersing the data they collect about their consumers.[97] For example, on February 9, 2011, Google, Inc. débuted a social

90. Cliff Edwards & Michael Riley, *Sony Data Breach Exposes Users to Years of Identity-Theft Risk*, BUSINESSWEEK (May 3, 2011), http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years-of-identity-theft-risk.html.

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* Michael Pachter, an analyst with Wedbush Securities in Los Angeles, estimated $50 million in damage to Sony during an interview with Bloomberg Television. *Id.* He based this figure on the credit-card fraud, repairs to network security, and marketing campaigns. *Id.*

95. Mathew J. Schwartz, *Sony Data Breach Cleanup to Cost $171 Million*, INFORMATIONWEEK (May 23, 2011), http://www.informationweek.com/news/security/attacks/229625379.

96. Strickling, *supra* note 5.

97. Berger, *supra* note 81, at 22.

networking site, called Google Buzz.[98] Prior to notice or consent, Gmail users were automatically set up with an instant network of friends based on their most frequently contacted email addresses and chat exchanges.[99] Google explained that this feature was intended to make it easy for users to get started with the new service, but promptly came up with alternative defaults and opt-out options when Google Buzz became a "privacy disaster."[100] While Google Buzz's privacy breach occurred while attempting to provide a service to its existing customers, other companies often sell user data to other companies that then use the data for marketing or advertising unrelated to the original company.[101]

2. Breach of Privacy: A Harm Itself

A breach of data privacy constitutes a harm itself. The assault to a user's personality and feelings is a privacy injury, brought on by an unauthorized acquisition of personal information.[102] This theory is buttressed by the concept of legal injury, one of the main principles of Warren and Brandeis' article: "[i]f the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."[103] Thus, the authors secured mental harm as a recognizable component of legal harm.[104] The existence of user

98. In re Google Inc., No. 102-3136, 2011 WL 1321658, *1, *2 (F.T.C. Mar. 30, 2011).

99. *Id.*

100. Nick Bilton, *Privacy Isn't Dead. Just Ask Google+*, N.Y. TIMES (July 18, 2011), http://bits.blogs.nytimes.com/2011/07/18/privacy-isnt-dead-just-ask-google/.

101. Berger, *supra* note 81, at 22-23.

102. Jay Cline, *When Does a Privacy Breach Cause Harm?*, COMPUTERWORLD (Mar. 6 2008), http://www.computerworld.com/s/article/9066958/When_does_a_privacy_breach_cause_harm_. Professor Anita Allen, of the University of Pennsylvania's law school, explained that breaches of privacy that injure one's personality or feelings are "the quintessential privacy injury." *Id.*

103. Warren & Brandeis, *supra* note 19, at 213.

104. *Id.* at 197-98.

profiles, detailing activities and what can be inferred from them, put users in danger of losing the ability to keep personal details private from those who want to use the data as a marketing tool.[105] Moreover, this sensitive information exists outside the user's control to protect or monitor it.[106]

Lists of seemingly benign email addresses can cause harm, given that users often re-use usernames and email addresses for various purposes. For instance, a list of email addresses could provide a missing link in aggregated data that could permit the identification of users and subvert the steps they took to preserve their online anonymity, such as in the case of Wikileaks, a controversial whistle-blowing website. The website accidentally leaked its own donors' email addresses by addressing a fundraising request email without using the blind carbon copy feature.[107] Then, someone submitted the revealing email as a leaked document to Wikileaks, and Wikileaks published it.[108] The social stigma and emotional suffering for the donors may have additional ramifications as Wikileaks became the target of investigation by the Department of Justice.[109] An unauthorized release of a name could also harm an individual depending on the context. For example, having one's name exposed on a list of HIV patients

---

However painful the mental effects upon another of an act, though purely wanton or even malicious, yet if the act itself is otherwise lawful, the suffering inflicted is *damnum absque injuria* [loss without damage]. Injury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as legal injury, but our system . . . does not afford a remedy even for mental suffering which results from mere contumely and insult, from an intentional and unwarranted violation of the 'honor' of another.
Id.

105. Berger, *supra* note 81, at 18.

106. *Id.* at 19.

107. Ryan Singel, *Wikileaks Forced to Leak Its Own Secret Info – Update*, WIRED (Feb. 18, 2009, 6:28 PM), http://www.wired.com/threatlevel/2009/02/wikileaks-force/.

108. *Id.* The publication of the email also contained a note, suggesting that the email was submitted to test the organization's principles of complete impartiality and objectiveness regarding whistleblowers. *Id.*

109. *See* Editorial, *The Justice Department Weighs a Criminal Case Against WikiLeaks*, THE WASH. POST (Aug. 18, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/17/AR2010081705225.html.

could expose an individual to a socially devastating stigma, employment problems, and general discrimination.

A user could also suffer embarrassment from the unintended disclosure of personal or private information.[110] For example, a Massachusetts Institute of Technology (MIT) class project analyzed 4,080 Facebook[111] profiles from the MIT network.[112] The MIT researchers were able to predict, with 78 percent accuracy, whether or not a profile belonged to a gay male.[113] The project authors explained that "although we studied Facebook friendship ties, network data is pervasive in the broader context of computer-mediated communication, raising significant privacy issues for communication technologies to which there are no neat solutions."[114] While all the profiles studied in the MIT class project may not have belonged to secretly homosexual males, the project illustrates that is has become easier to identify character traits of users from non-descriptive data.

An individual's information is more readily available as seemingly anonymous data is continually linked and merged from different databases, building more detailed user profiles.[115] Furthermore, in touting Google's image-search technology, former Google executive Eric Schmidt explained that "[i]f you have 14

110. Berger, *supra* note 81, at 19.

111. *About*, FACEBOOK, http://www.facebook.com (last visited Oct. 26, 2011). In its privacy policy, Facebook states that it does share aggregated information with third parties, such as advertisers, in order to improve their product, or for promotion. *See Information We Receive and How It Is Used*, FACEBOOK.COM, http://www.facebook.com/about/privacy/your-info (last visited Oct. 26, 2011). Facebook also explains that it aggregates "data from the information we already have about you and your friends." *Id.* Facebook acknowledges sharing user information, with "advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you." *Id.*

112. Jernigan & Mistree, *supra* note 54. First Monday is a peer–reviewed Internet-based journal. *See Editorial Policies*, FIRST MONDAY, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/about/editorialPolicies#peerReviewProcess (last visited Oct. 22, 2011).

113. Jernigan & Mistree, *supra* note 54.

114. *Id.*

115. BALLON, *supra* note 7.

pictures on the Internet, within a 95% confidence interval we can predict who you are. You say you don't have 14 pictures? You have Facebook pictures, so there."[116] Our modern technological society, with social networking sites and online accounts, has created an enormous body of personally identifiable information readily available for capture.[117] In a worst-case scenario, behavioral data profiles could be used inappropriately, to target users with controversial interests, or to establish differential pricing for goods or services.[118]

Embarrassment and discrimination can also lead to physical harms. For instance, the widespread availability of PII can facilitate criminal stalking. In *U.S. v. Rodriguez*, the court affirmed the conviction of the defendant, a former federal employee of the Social Security Administration, for illegally obtaining the PII of 17 people, pursuant to the Computer Fraud and Abuse Act.[119] Most of the defendant's victims testified at trial about his intrusion into their personal lives, through unwanted advances, gifts, phone calls, and long-distance, unannounced visits.[120] In affirming the defendant's conviction, the court emphasized the "unwelcomed" manner in which he used the information.[121] While in this case the emotional torment of the defendant's victims did not progress to in physical assaults, the

116. Courtney Banks, *Top 10: The Quotable Eric Schmidt*, THE WALL STREET JOURNAL (Jan. 21, 2011), http://blogs.wsj.com/digits/2011/01/21/top-10-the-quotable-eric-schmidt/.

117. *See generally* PETER LYMAN & HAL R. VARIAN, HOW MUCH INFORMATION? 2003, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf (last visited August 7, 2011). According to the Executive Summary of the U.C. Berkeley study, 99.99% of information is currently being created in electronic form. *Id.*

118. Berger, *supra* note 81, at 20. For instance, the author explains that insurers or creditors could use a consumer's profile in an attempt to establish individual-specific pricing based on their behavior (i.e., threat). *Id.*

119. United States v. Rodriguez, 628 F.3d 1258, 1265 (11th Cir. 2010). *See also* the Computer Fraud and Abuse Act (CFAA), codified in 18 U.S.C. § 1030(a)(2)(B) (2006).

120. *Id.* at 1261-62. One victim, a professor of sociology, had her information accessed 65 times. *Id.* at 1261. Her parents' personal information was also accessed. *Id.*

121. *Id.* at 1265.

potential exists. In 2002, Amy Boyer was murdered by a former classmate, who obtained her PII from an online information broker.[122] Armed with a gun and Boyer's information, the classmate tracked Boyer, and shot her as she left work.[123] Some lawmakers have begun to recognize the connection between unauthorized collection of personally identifying information and the potential for physical harm,[124] and enacted stalking statutes to penalize the conduct.

D. The Dialogue About Online Privacy Regulation

The proposed DNT Bills were introduced in response to the dialogue between the online advertising industry and the FTC. The FTC has privacy enforcement authority under several statutes, including protections for financial privacy,[125] the privacy of credit information,[126] and the privacy of personally identifiable information relating to children.[127] The FTC's Bureau of Consumer Protection (BCP) regulates matters involving online consumer privacy.[128] The FTC established an office, the Division of Privacy and Identity Protection, specifically intended to protect online consumer privacy, ensure information security, and combat

122. Robert O'Harrow, Jr., *Online Firm Gave Victim's Data to Killer*, CHI. TRIB. (Jan. 6, 2002), http://articles.chicagotribune.com/2002-01-06/news/0201060305_1_pretexting-docusearch-amy-boyer. Docusearch used online database services to aggregate public-record information about individuals, including Social Security numbers, telephone numbers, and other personal details. *Id.* The classmate only paid $150 to obtain Boyer's PII. *Id.*

123. *Id.*

124. WIS. STAT. § 940.32(2m) (2011). Wisconsin classified a stalker gaining access or causing another person to gain access to a record in electronic format, which contains the victim's personally identifiable information, as a Class H felony. *Id.*

125. *See* 15 U.S.C. § 6805 (2006) (granting the FTC authority to enforce Gramm-Leach-Bliley Act requirements as to financial institutions not subject to the jurisdiction of other federal agencies or state insurance authorities).

126. *See* 15 U.S.C. § 1681s(a) (2006).

127. *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6502 (2006).

128. *About the Bureau of Consumer Protection*, OFFICES AND BUREAUS, http://www.ftc.gov/bcp/about.shtm (last modified June 16, 2009).

identity theft.[129] In other subject areas, the FTC has taken a broad view of its role under Section 5 of the Federal Trade Commission Act (FTCA), which empowers the FTC to investigate "unfair or deceptive acts or practices in or affecting commerce."[130]

Beginning in the late 1990's, the FTC filed complaints against various companies, treating breaches of privacy policies as unfair and deceptive trade practices under Section 5.[131] Enforcement actions included filing complaints against companies that violated their own privacy policies, often by breaching promises to not publicly share personally identifying information,[132] and breaches of promises to safeguard customers' information.[133] Recently, the

129. *Division of Privacy & Identity Protection*, FTC BUREAU OF CONSUMER PROTECTION, http://www.ftc.gov/bcp/bcppip.shtm (last modified Oct. 23, 2007).

130. *Legal Authority*, GENERAL COUNSEL, http://www.ftc.gov/ogc/brfovrvw.shtm (last modified July 2, 2008). The statute authorizes the FTC to protect consumers by prohibiting "unfair or deceptive acts or practices in or affecting commerce," in addition to "[u]nfair methods of competition." 15 U.S.C. § 45(a)(1) (2006). Subsection (n), titled *Standard of Proof; public policy consideration*, states in full:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

Id. § 45(n).

131. *See* 15 U.S.C. § 45.

132. *See* Complaint at 2, FTC v. Toysmart, LLC, No. 00-11341-RGS, 2003 WL 34016434 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm.

133. *See* Complaint at 3, In re Eli Lilly & Co., No. C-4047, 2001 WL 1712505 (F.T.C May 8, 2002). The FTC asserted that Eli Lilly represented that it employed measures and took steps to ensure the privacy of their customers' personal information, but such claims were false. *Id. See also* In re Google Inc., No. 102-3136, 2011 WL 1321658, at *1 (F.T.C. Mar. 30, 2011). The FTC found that Google did not use information from consumers strictly for the

FTC has interpreted Section 5 of the FTCA as directly obligating companies to safeguard personally identifying information, regardless of whether the company's privacy policy promises to protect it.[134] However, the FTC's enforcement power is limited to addressing breaches of privacy in the context of fair business practices, not the invasion of personal privacy.[135]

After a decade of studying the impact of Internet advertising on user privacy, the FTC released its Guidelines for Self-Regulation in Online Behavioral Advertising (FTC Guidelines) in February 2009.[136] The agency recognized that users have legitimate concerns about the collection and storage of data regarding their online activities, but the agency also recognized that consumers receive the benefit of free access to online material that advertising supports.[137] For more effective privacy controls, the FTC advised that companies clearly disclose their privacy policies, take reasonable data security measures, obtain users' express consent before using their collected data in a manner "materially different" than disclosed, and obtain the express consent of users before using sensitive data, such as health or financial information, for behavioral advertising.[138] FTC Commissioner Jon Leibowitz declared that the online advertising industry should regard the agency's guidelines as its "last clear chance to show that self-regulation can—and will—effectively protect consumers' privacy

---

purpose of providing them with an email service, which contradicted Google's express and implied representation of data use. *Id.* at *5.

134. In re TJX Co.s, No. C-4227, 2008 WL 3150421, at *1-2 (F.T.C. July 29, 2008). The FTC filed a complaint alleging that TJX failed to employ "reasonable and appropriate security measures to protect personal information," and as a result, caused the risk of substantial financial harm to consumers. *Id.* at *1. The FTC did not allege that TJX violated specific FTC rules or its own policies, but instead viewed TJX's failure to safeguard customer data as an unfair trade practice itself. *Id.*

135. Brill, *supra* note 4, at *2.

136. FTC GUIDELINES, *supra* note 77.

137. *Id.* at 1.

138. *Id.* at 11-12. The FTC urged the industry to take ownership of the self-regulatory model by requiring compliance with the Guidelines, and ensuring that violations have consequences. *Id.* at 47.

in a dynamic online marketplace."[139] Leibowitz also reminded the industry that it "needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission."[140]

In response to the FTC Guidelines, the online advertising industry[141] compiled their own self-regulatory model (Industry Guidelines), setting forth principles corresponding to the FTC's guidelines.[142] Despite these self-regulatory efforts, privacy advocates argued that they were insufficient, and the best way to protect users' privacy in a dynamic arena was for the United States to adopt a comprehensive framework like the European Union's (E.U.'s) approach to privacy.[143]

Subsequently, the FTC addressed what it felt was the industry's lack of progress in protecting user's online privacy, and proposed

139. Concurring Statement of Commissioner Jon Leibowitz, Chairman of the Fed. Trade Comm'n (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.

140. *Id.*

141. *See The Self-Regulatory Program for Online Behavioral Advertising,* DIGITAL ADVERTISING ALLIANCE, http://www.Aboutads.info/principles (last visited Oct. 26, 2011). The Principles were formed by the online advertising industry's self-regulatory guidelines in response to the FTC's guidelines. *Id.* The participating organizations include: American Association of Advertising Agencies, Association of National Advertisers, the Council of Better Business Bureaus, Direct Marketing Association, and Interactive Advertising Bureau. *Participating Associations,* DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info/associations (last visited Oct. 26, 2011).

142. *The Self-Regulatory Principles for Online Behavioral Advertising,* DIGITAL ADVERTISING ALLIANCE, 2-4 (July 2009), http://www.Aboutads.info/resource/download/seven-principles-07-01-09.pdf. The Industry Guidelines set forth seven guiding principles: (1) transparency of policies for data collection and use; (2) mechanisms for user control and opting out of collection; (3) reasonable data security measures; (4) notification of material changes in privacy policies; (5) enhanced protection of sensitive data; (6) consumer education; and (7) accountability. *Id.* at 1-4.

143. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 11-12 (2010) [hereinafter GREEN PAPER] http://www.ntia.doc.gov//reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf. The E.U.'s overarching approach to privacy is in contrast to the United States' piecemeal approach to privacy and emphasis on free speech. *Id.*

three ways companies could improve their privacy practices: adopt a specific privacy policy based on daily operations, make their data security and practices more transparent to users, and provide users with meaningful choices of opting out of data collection.[144] To make website operators aware of a user's preference to opt out, a "Do Not Track" tool could signal to website operators whether or not the user wants to be tracked or receive targeted advertisements.[145] An opt-out tool could be accomplished by either legislation or enforceable self-regulation.[146] Thus, the FTC reiterated that DNT legislation is not the only solution; rather, "robust, enforceable self-regulation" could be effective in controlling privacy data, so long as there are consequences for websites that do not adhere to users' opt-out preferences.[147]

III. THE CURRENT PROPOSED LEGISLATION

This section introduces the two proposed Do Not Track (DNT) Bills, both setting forth provisions for an opt-out policy to protect user's informational privacy.

A. H.R. 654: Do Not Track Me Online Act

Representative Jackie Speier, of the House Energy and Commerce Committee, felt that to date, efforts to protect online

144. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS i, iv-vii (Dec. 2010), http://ftc.gov/os/2010/12/101201privacyreport.pdf. The agency proposed that companies aim to present their practices in clear terms, and consumer choice would not be necessary for "commonly accepted" data practices, such as legal compliance, first-party marketing, and order completions. *Id.* at vi. This would allow users a more "meaningful choice" about atypical practices. *Id.* at vii.

145. *Id.* at 66.

146. *Id.*

147. *Id.*

privacy have been ineffective.[148] In response, she introduced the Do Not Track Me Online Act on February 11, 2011, which directs the FTC to prescribe regulations regarding the collection and use of information derived from tracking users' Internet activity.[149] After the Bill was introduced, it was referred to the House Subcommittee on Commerce, Manufacturing, and Trade.[150]

Section 2 sets forth definitions relative to the enforcement of the Act. It defines a "covered entity" as "a person engaged in interstate commerce that collects or stores data containing covered information," and does not include the federal, state, or local governments.[151] "Covered information" is broadly defined as information transmitted online, such as the online activity of an individual, including websites and content, date, time, geolocation of the accessing device, and device type.[152] "Covered information" also includes any unique identifier, such as a customer number or IP address, name, postal address, email address, phone number, or financial account numbers.[153]

Section 3 authorizes FTC rulemaking authority and sets forth some requirements to be included in the regulations. The FTC would have the right to propose regulations for the collection and use of information obtained by tracking user Internet activity.[154] Prescribed regulations would be given the same effect as those affecting unfair and deceptive acts involving commerce pursuant to the Federal Trade Commission Act.[155] Subsection (B) briefly outlines two requirements for regulations. First, covered entities

148. Grant Gross, *Lawmaker Introduces Online Do-Not-Track Bill*, COMPUTERWORLD (Feb. 11, 2011), http://www.computerworld.com/s/article/9209178/Lawmaker_introduces_online_do_not_track_bill.

149. Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(a)-(c) (2011).

150. *Bill Summary and Status 112th Congress H.R. 654*, THE LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR00654:@@@L&summ2=m& (last visited Nov. 21, 2011). The bill went to Subcommittee on February 18, 2011. *Id.*

151. H.R. 654 § 2(2).

152. *Id.* § 2(3)(A)(i).

153. *Id.* § 2(3)(A)(ii)-(iii).

154. *Id.* § 3(a).

155. *Id.* (citing 15 U.S.C. § 57a(a)(1)(B) (2006)).

must disclose data collection practices and uses.[156] Second, a covered entity must respect the choice of the user who elects to opt out of data collection for covered information.[157] Subsection (C) sets forth two optional provisions of providing consumers with a means to access covered information, and that some or all of the regulations apply regarding of the source of the data.[158] Subsection (D) provides for some commonly accepted commercial services to be exempt from the opt-out policy, including: (1) providing, operating, or improving a product or service used, requested, or authorized, (2) protecting or defending rights or property against security threats, fraud, theft, unauthorized transactions, or other illegal activities; and (3) preventing imminent danger.[159] For example, the collection of data for billing purposes or order fulfillment would be allowed, but the companies would need to disclose their collection and sharing practices.[160]

Section 4 outlines additional FTC authority in implementing and enforcing regulations. The FTC must monitor products that might circumvent consumers' abilities to control data collection, and audit covered entities for compliance.[161] Annually, the FTC must report significant findings of product risks to consumers.[162]

Section 5 states that companies and websites that do not honor the opt-out request would be subject to unfair or deceptive practice complaints, enforced by the FTC, or enforcement actions by states' attorneys general.[163] However, the Bill does not provide for a private right of action.[164] Section 6 specifies that the Bill does not preempt state law.[165]

156. Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(b)(1) (2011).
157. *Id.* § 3(b)(2).
158. *Id.* § 3(c)(1)-(2).
159. *Id.* § 3(d) (1)-(7).
160. *Id.* § 3(d).
161. *Id.* § 4(2)-(3).
162. Do Not Track Me Online Act, H.R. 654, 112th Cong. § 4(5) (2011).
163. *Id.* § 5.
164. *See generally* H.R. 654.
165. *Id.* § 6(b).

B. S. 913: Do-Not-Track Online Act of 2011

Senator Jay Rockefeller, Chairman of the Senate Committee on Commerce, Science and Transportation, proposed the Do-Not-Track Online Act of 2011, which requires the FTC to prescribe regulations regarding the collection and use of personal information, obtained from the online tracking of users' activity.[166] After this Bill was introduced, it was referred to the Senate Committee on Commerce, Science, and Transportation.[167]

Like House Bill 654 described above, this Act purports a browser-based DNT mechanism to allow users to opt out of having their online information monitored and collected.[168] Section 2 sets forth the regulations relating to the DNT mechanism. The FTC must establish standards for the implementation of a mechanism which indicates a user's preference for data collection of personal information by online services.[169] However, the Bill does not define the term "personal information"; rather, it provides that the FTC will establish standards for the implementation of a mechanism and in doing so, will have to define the term.[170] The Bill also requires companies to respect a consumer's choice to opt out of data collection.[171] However, the Bill would allow for the collection of user data in order to provide a service as requested by the user, and then delete or anonymize the data upon completion.[172] Unlike the House proposed legislation, this Bill applies to mobile phone applications.[173] In promulgating the DNT regulations, the FTC would be able to consider mechanisms already developed as well as evaluating the technical feasibility and associated costs.[174]

166. *See* Do-Not-Track Me Online Act of 2011, S. 913, 112th Cong. (2011).

167. *Bill Summary and Status 112th Congress S. 913*, THE LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00913:@@@L&summ2=m& (last visited Nov. 21, 2011).

168. S. 913 § 2(a)(1)-(2).

169. *Id.* § 2(a)(1).

170. *Id.*

171. *Id.* § 2(a)(2).

172. *Id.* § 2(b).

173. *Id.* § 2(a)(1).

174. Do-Not-Track Me Online Act of 2011, S. 913, 112th Cong. § 2(c)(1)-(2) (2011).

The FTC is also instructed to consider the simplicity and ease with which users can utilize the mechanism.[175]

Section 3 sets forth the enforcement provisions. Without a private right of action, enforcement of the DNT mechanism would be primarily the responsibility of the FTC, pursuant to the Federal Trade Commission Act.[176] Violations of a rule promulgated by the FTC will be treated as an unfair or deceptive act, but the FTC will not be able to enforce civil penalties.[177] The states' attorneys general can enforce the law, but the FTC would retain the right to intervene.[178] The Bill does not provide federal preemption of state laws.[179] Section 4 calls for a biennial report and assessment of the implementation of the Act, the effectiveness of the regulations in interpreting "personal information," and the effect of the regulations on online commerce.[180]

IV. ANALYSIS

This section will explore the effects of Do Not Track (DNT) legislation on online privacy. First, this section will discuss how these Bills do not fill the gap in current privacy protection because they are ineffective at providing universal protection and enforcement. Then, this section will examine the potential negative impact of implementation, including the loss of free and customized Internet content. This section concludes with a survey of the technical problems of DNT implementation.

A. Attempting to Fill the Gaps

Due to the categorization of United States' privacy laws by subject matter, there is no single agency dedicated to protecting

175. *Id.* § 2(c)(3).
176. *Id.* § 3. *See* 15 U.S.C. § 41 (2006).
177. *Id.* §§ 3(a)(1), (a)(2)(A).
178. *Id.* §§ 3(b)(1), (b)(3)(B).
179. *See id.* §§ 3(b)(1), (b)(3)(B).
180. Do-Not-Track Me Online Act of 2011, S. 913, 112th Cong. § 4 (2011). The report should be submitted to Congress. *Id.*

informational privacy,[181] nor is any Internet company legally required to uphold customers' privacy requests.[182] Generally the FTC and the Federal Communications Commission (FCC) can address breaches of privacy, but the context of the breaches must reside in enforcing fair business practices, not the invasion of personal privacy.[183]

The DNT legislation grants the FTC and states' attorney generals enforcement power in the data privacy context, but it does not close the existing gaps in privacy laws because it fails to establish universal protection for all users on the Internet, and does not provide greater enforcement due to a lack of a private right of action.

The abundance of privacy-related proposed legislation currently in Congress suggests that "a consensus has formed in Washington that the patchwork of federal and state privacy laws have not kept pace with the development of the Internet. The U.S. lags behind Europe, where broad safeguards of personal digital information have been in place since 1995."[184] The European Union's (E.U.'s) Privacy Directive recognizes that data privacy is a fundamental human right, and regulates the use of personal data.[185] The Directive stipulates that personal data cannot be processed, unless necessary, without the users' consent, and users maintain the right to access, edit and object to the mined information.[186] Furthermore, websites that collect user information must disclose their practices to users.[187] E.U. regulatory bodies monitor a

181. James Kanter, *Europe Leads in Pushing for Privacy of User Data*, N.Y. TIMES (May 3, 2011), http://www.nytimes.com/2011/05/04/technology/04iht-privacy04.html.

182. Cecilia Kang, *Sen. Rockefeller Introduces 'Do Not Track' Bill for the Internet,* WASH. POST (May 9, 2011), http://www.washingtonpost.com/blogs/post-tech/post/sen-rockefeller-introduces-do-not-track-bill-for-internet/2011/05/09/AF0ymjaG_blog.html.

183. *See* the Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(B) (2006).

184. Forden, *supra* note 58.

185. BALLON, *supra* note 7. Many of the guiding concepts from the E.U. Directive influenced the FTC Guidelines on privacy issues as the agency made privacy one of its main focuses. *Id.*

186. *Id.*

187. *Id.*

registration system that harmonizes privacy laws throughout the Union.[188] The increasing use of the Internet in commerce, along with the E.U.'s adoption of the Privacy Directive, prompted U.S. legislators to find a solution to allow U.S. businesses to transfer data from Europe.[189]

The patchwork of U.S. privacy laws tend to protect specific categories of information, or individuals in specific circumstances. For instance, the Cable Act and the Communications Act prohibit cable and phone companies offering telephone service from freely disclosing their customers' locations, but Section 2702 of the Electronic Communications Privacy Act allows smartphone companies, application companies, and wireless service companies to freely share customers' locations without consent.[190] Furthermore, except for personal information from financial services or healthcare companies, data privacy laws generally are not governed by federal statutes.[191] For instance, the Gramm-Leach-Bliley Act imposed specific legal obligations on companies to maintain the security of data in the financial services industry.[192] Likewise, the Health Insurance Portability and Accountability Act (HIPAA) required the implementation of extensive safeguards to maintain the confidentiality and integrity of electronic data maintained in the health care industry.[193] The Sarbanes-Oxley Act requires information security standards for publicly traded companies, but the Act does not expressly define those measures.[194]

Another federal privacy act, the Children's Online Privacy Protection Act of 1998 (COPPA), does not focus on a subject

---

188. *Id.*

189. *Id.*

190. THE LOCATION PRIVACY PROTECTION ACT OF 2011 (S. 1223) BILL SUMMARY (June 14, 2011), *available at* http://franken.senate.gov/files/docs/110614_The_Location_Privacy_Protection_Act_of_2011_One_pager.pdf.

191. BALLON, *supra* note 7. Ballon explains that California and Texas lead the way in protecting data privacy, by adopting laws that affect nationwide companies. *Id.*

192. *See* 15 U.S.C. §§ 6801-6809, 6821-6827 (2006).

193. *See* 42 U.S.C. §§ 1320d *et seq.* (2006).

194. *See* 15 U.S.C. § 7241 (2006).

matter but instead, focuses on a specific group that may be harmed by a privacy breach.[195] Pursuant to the Act, without express consent from a parent or guardian, a website operator cannot collect identifying information from a child online,[196] including name, address, email address, telephone number, or Social Security number.[197] Legislators sought to protect children's anonymity and safety because children lacked the ability to perceive the potential harms from giving out personal information over the Internet.[198]

Congress authorized the FTC to enforce actions and impose civil penalties for violations of COPPA in the same manner as for other rules defining unfair or deceptive acts or practices pursuant to Section 5 of the Federal Trade Commission Act,[199] and the FTC has brought successful actions against website operators for failing to comply with COPPA.[200] One gap in COPPA protection is that it does not protect Internet users over the age of thirteen, and recent studies have revealed that 71 percent of teenagers use the Internet for social networking purposes.[201] Teenagers may be aware that

195. *See* 15 U.S.C. § 6502 (2006).

196. 15 U.S.C. § 6502(a).

197. 15 U.S.C § 6501(8) (defining "personal information").

198. Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW J. L. & SOC. POL'Y 369, 369 (2010).

199. *Id.* § 6505(a)-(e). *See also* 15 U.S.C. § 6502(c) (providing that the rule shall be treated as a rule issued under § 18(a)(1)(B) of the FTC Act, codified as 15 U.S.C. § 57a(a)(1)(B) (2006)). States' attorneys general are also authorized to bring civil actions on behalf of state citizens who were "threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under [COPPA]." 15 U.S.C. § 6504(a)(1) (2006).

200. *See* Consent Decree & Order at 6, United States v. Playdom, Inc., No. SACV11-00724-AG (C.D. Cal. May 11, 2011), *available at* http://www.ftc.gov/os/caselist/1023036/110512playdomconsentorder.pdf. In addition to the $3 million penalty, the settlement permanently barred the company from violating COPPA and from misrepresenting its information practices regarding children. *Id.* at 4-6.

201. Matecki, *supra* note 198, at 370. Some critics have also argued that COPPA encourages website operators to ban users under thirteen, and in effect, leads to age fraud. *Id.* Furthermore, by excluding children under thirteen,

collection of personal information occurs online, but may not appreciate the associated risks.[202] Thus, despite some successful privacy protection under COPPA, teenagers and adults are still susceptible to online surveillance.

The FTC is limited to addressing breaches of privacy in the context of enforcing fair business practices, not the invasion of personal privacy.[203] Although the DNT legislation grants the FTC explicit enforcement power, it does not close the existing gaps in privacy laws because, as examined in the following sections, it fails to establish universal protection for all users on the Internet since the FTC is still confined to enforcing fair business practices. Furthermore, it does not provide greater enforcement power due to a lack of a private right of action.

1. Universal protection

The DNT legislation does not provide universal protection for users on the Internet because it fails to establish protection for Internet users outside of the fair business practices context, as limited by the Federal Trade Commission Act.[204] Furthermore, the Bills likely do not affect terms of service agreements.

The Bills authorize the FTC to promulgate rules, enforce actions, and impose civil penalties for violations in the same manner as for other rules defining unfair or deceptive acts or practices pursuant to Section 5 of the Federal Trade Commission Act.[205] According to statements by Bill supporters, this solves the problem of universal protection for all consumers. Rep. Speier's stated goal of House Bill 654 was to employ a straightforward, universal mechanism because currently there are no legal limitations on how companies track consumers online, and the Bill

---

websites subvert the intent of COPPA by bypassing the burden of obtaining parental consent. *Id.*

202. Brill, *supra* note 4, at *2.

203. *See* Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(B) (2006).

204. *See id.*

205. *See* Do-Not-Track Me Online Act of 2011, S. 913, 112th Cong. § 3(a)(1) (2011), and Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(a) (2011) (providing that the rule shall be treated as a rule issued under the Federal Trade Commission Act (15 U.S.C. § 57a(a)(1)(B) (2006))).

"will allow consumers to make a basic choice that they think they already had."[206] Sen. Rockefeller reiterated that "consumers have a right to know when and how their personal and sensitive information is being used online—and most importantly to be able to say 'no thanks' when companies seek to gather that information without their approval."[207]

House Bill 654 attempts to accomplish this goal by directing the FTC to create standards for a nationwide DNT mechanism that allows users to opt out of all online data collection.[208] The Bill applies uniformly to all "covered entities," defined as persons engaged in interstate commerce, and collects or stores data containing covered information, and does not include the federal, state or local governments.[209] The Bill also broadly defined "covered information," as any information transmitted online, such as the online activity of an individual, including websites and content, date, time, geolocation of the accessing device, and device type.[210] "Covered information" also extended to include any unique identifier, such as a customer number or IP address, name, postal address, email address, phone number, or financial account numbers.[211]

Senate Bill 913 also proposes a browser-based DNT mechanism to allow users to universally opt out of all data collection across the Internet.[212] However, the Bill does not define the terms "personal information" or "covered entities," and instead stipulates that the FTC will define the terms along with developing standards for the implementation of a user-friendly browser-based mechanism.[213] Both the Bills bring DNT regulation under Section

206. Gross, *supra* note 148.

207. Tanza Vega, *'Do Not Track' Privacy Bill Appears in Congress*, N.Y. TIMES (May 6, 2011), http://mediadecoder.blogs.nytimes.com/2011/05/06/do-not-track-privacy-bill-appears-in-congress/.

208. H.R. 654 § 3(a)-(c).

209. *Id.* § 2(2).

210. *Id.* § 2(3)(A)(i).

211. *Id.* § 2(3)(A)(ii)-(iii).

212. S. 913 § 2(a)(1)-(2).

213. *Id.* § 2(a)(1).

5 of the Federal Trade Commission Act,[214] but they do not expand the FTC's ability to enforce privacy breaches in a general context. Furthermore, it is unclear what rights it purports for users who suffer a breach of informational privacy, not involving interstate commerce. The tracking of user data does not occur exclusively within the interstate commerce framework, but can occur during any type of online activity. Moreover, House Bill 654 excludes from the "covered entity" category any person who fulfills the following criteria: "(1) stores covered information from or about fewer than 15,000 individuals, (2) collects covered information from or about fewer than 10,000 individuals annually, (3) does not collect or store sensitive information, and (4) does not use covered information to monitor or analyze users' online activity as a primary business.[215] Therefore, a smaller-sized tracking company would not qualify as covered entity if it fell within the statutory limits, and would not be regulated by the DNT Bills. Yet, that small company is certainly capable of the dissemination of personal information and causing harm. This DNT legislation cannot be considered universal protection when it includes easily-filled exclusions.

Many governmental agencies seem to favor industry self-regulation over a comprehensive DNT bill, due to the complexity of monitoring and regulating data privacy online, and the difficulty of establishing a universal approach. The Obama Administration stated that cybersecurity must be a priority in order to ensure that cyberspace is capable of supporting economic growth, protecting civil liberties and privacy, and national security.[216] The

214. *See* S. 913 § 3(a)(1) and H.R.654 § 3(a), providing that the rule shall be treated as a rule issued under § 18(a)(1)(B) of the FTC Act (15 U.S.C. § 57a(a)(1)(B)).

215. H.R. 654 § 2(2)(B).

216. Press Release, Office of the Press Sec'y, The White House, Fact Sheet on Cyberspace Policy Review: Assuring a Trusted and Resilient Info. and Commc'ns Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees. The Administration's support for privacy is significant because it is the first time in over 30 years that the Federal government has supported mandatory privacy regulation. Jaikumar Vijaya, *Obama Administration Calls for New Privacy Law*, COMPUTERWORLD (Mar. 16, 2011), http://www.computerworld.com

Administration advised that due to the complex, interdependent, privatized communications industry, "no single, integrated vision exists to guide decision-making by the private sector, academia, and government about policies, standards, research, [or] market development."[217] Thus, a DNT bill would seem to go against the recommendation that no single authority effectuate online privacy protection. The Subcommittee on Privacy and Internet Policy,[218] established to promote the Administration's privacy goals, oversees the efforts addressing privacy issues and develops approaches to foster dialogue and cooperation between the government and companies.[219] The task force also works on transforming the Commerce Department's recommendations into policy.[220] It is unclear how the DNT legislation will affect or circumvent the Subcommittee's efforts, as the FTC does not have a seat on the task force.[221]

The Commerce Department also called for stronger privacy regulation through a multi-stakeholder approach, in its 2010 Green

/s/article/9214684/Obama_Administration_calls_for_new_privacy_law. The last time support to this extent was seen was for the U.S. Data Privacy Act of 1974, a broad privacy rule. *Id.* The Act was originally meant to encompass both the private and public sectors, but it was revised before enactment to apply to only government agencies. *Id. See also* U.S. Data Privacy Act of 1974, 5 U.S.C. § 552(a) (2006).

217. THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 32 (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

218. Kerry & Schroeder, *supra* note 6. To facilitate the Obama Administration's focus on promoting Internet economic opportunities and protecting individual privacy, the National Science and Technology Council (NSTC) created a new Subcommittee on Privacy and Internet Policy, including of members from the following Departments of Commerce, Justice, Education, Energy, Health and Human Services, Homeland Security, State, Transportation, and Treasury. *Id.* The Subcommittee is led by Christopher Schroeder, Assistant Attorney General at the Department of Justice, and Cameron Kerry, General Counsel of the Commerce Department. *Id.* The FTC and Federal Communications Commission (FCC) are not represented on the Subcommittee. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

Paper report.[222] The Green Paper recognized that in the past, subject-specific legislation and the FTC's enforcement power work well to protect consumers' privacy.[223] However, the Green Paper outlined how federal laws regulating companies' data collection practices could be updated, and acknowledged that there were areas where the law was deficient.[224] It called for a new dynamic approach to remedying gaps in privacy protection, which included the advertising industry's participation.[225] Privacy regulation should not come at the expense of stifling technological advancement.[226] The proposed DNT Bills do not fulfill the Commerce Department's or the Obama Administration's suggested criteria of universal privacy control involving multiple stakeholders, because the Bills, on their surface, remove industry participation.

In March 2011, the Obama Administration restated its support for comprehensive consumer data privacy protections, but only within the commercial framework. The Administration called for legislation that would promote flexibility in regulating Internet privacy issues, due to the rapidly changing technological landscape.[227] To achieve strong privacy protection while encouraging innovation, the Administration offered three guidelines.[228] First, consumer protections should be flexible, enforceable at law, and serve as guides for developing codes of conduct for application of the legislative principles in the context of commerce.[229] Second, legislation should incentivize stakeholders to adhere to enforceable codes of conduct.[230] Finally, legislation should strengthen the FTC's consumer data privacy enforcement authority.[231] While these guidelines attempted to strengthen support for privacy protection overall, they are

222. GREEN PAPER, *supra* note 143, at iv.
223. *Id.* at 68.
224. *Id.* at 35-36.
225. *Id.* at 68-69.
226. *Id.* at 12, 68-69.
227. Strickling, *supra* note 5.
228. *Id.*
229. *Id.*
230. *Id.*
231. *Id.*

specifically focused on protecting consumers, not all online users. Like the DNT legislation, these guidelines do not reflect the susceptibility of users' online activities that are not within the interstate commerce context.

The DNT Bills also do not provide universal protection because they do not address the effect of terms of service agreements on users' ability to protect their privacy. For instance, if enacted, the Bills may not affect the profiling practices of Facebook, a first party user of data.[232] Facebook collects three types of information about its users: information provided for account registration,[233] information other Facebook users share about a user,[234] and information from user interactions on the website.[235] Facebook uses the information it collects for a variety of purposes, including suggesting services or features, and keeping a secure website.[236] The website also uses this data to measure the effectiveness of advertisements.[237] This is especially concerning as Facebook becomes a leader in online targeted advertising and serves as an access point to millions of users.[238] For instance, GraphEffect is launching an "intelligent targeting system," which is a platform that allows advertiser to target Facebook advertisements based on the behavioral characteristics that are not explicit in Facebook user log activity.[239] This new targeting method is different in that it identifies certain traits of Facebook users, including likes,

232. *Information We Receive and How It Is Used*, FACEBOOK.COM, http://www.facebook.com/about/privacy/your-info (last visited Oct. 26, 2011).

233. *Id.* This information includes a user's name, email address, birthday, and gender. *Id.*

234. *Id.* For example, Facebook collects information about a user when he is tagged in a photo or at a location, or added to a group. *Id.*

235. *Id.* For example, Facebook collects information when a user looks at person's profile, sends a message, searches for friends or a Page, or clicks on an advertisement on Facebook's website. *Id.* *See also* discussion on "click-through" technology, *supra* note 53.

236. *Information We Receive and How It Is Used*, *supra* note 232.

237. *Id.*

238. Leena Rao, *GraphEffect Launches Intelligent Facebook Advertising And Targeting Platform For Brands*, TECHCRUNCH (Aug. 19, 2011), http://techcrunch.com/2011/08/19/grapheffect-launches-intelligent-facebook-advertising-and-targeting-platform-for-brands/.

239. *Id.*

interests, and demographics, and creates "lookalike" models for brands to target.[240] Thus, social media websites, like Facebook, appear to be a technological loophole in the proposed DNT legislation, illustrating that the uniformity of protection from DNT legislation is questionable.

2. Enforcement

If Senate Bill 913 or House Bill 654 were enacted, users would not have means of enforcing their own rights against violators of their online privacy, unless the FTC or state's attorneys general decided to bring legal action. The lack of a private right of action undermines consumer enforcement power in the same way behavioral tracking undermines the intent of the user that wishes to browse the Internet anonymously. While the enforcement power of the DNT legislation is a step toward enforcing online privacy rights, it is ultimately ineffective because it omits a private right of action.

With the passage of DNT legislation, online companies could be held accountable for their breaches of users' opt-out preferences.[241] After all, some privacy advocates feel that "[t]here is no longer any anonymity on the Web—unless we mandate it."[242] For instance, House Bill 654 explicitly requires companies to respect the choice of the user who elects to opt out of data collection for covered information.[243] Companies and website operators that do not honor the opt-out request would be subject to unfair or deceptive practice complaints, enforced by the FTC, or enforcement actions by states' attorneys general.[244] However, the Bill does not provide for a private right of action.[245]

Likewise, Senate Bill 913 would also compel companies to respect a consumer's choice to opt out of data collection by

240. *Id.*

241. Jackie Speier, *Do Not Track Our Online Data*, POLITICO (Mar. 4, 2011), http://www.politico.com/news/stories/0311/50614.html.

242. *Id.*

243. Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. § 3(b)(2) (2011).

244. *Id.* §§ 4, 5.

245. *See generally* H.R. 654.

granting enforcement action to the FTC and the ability to impose civil penalties.[246] The states' attorneys general can enforce compliance with a user's DNT preference, under both state and federal law, but users do not have means of enforcing their own rights under the Bill.[247]

Thus, if Senate Bill 913 or House Bill 654 were enacted, affected consumers would not have statutory support for legal action against violators of their online privacy, unless the FTC or state's attorney decided to pursue action. This is problematic because governmental agency action is subject to funding constraints, manpower, the philosophy of the administrative power, and the magnitude of the offense.[248] "[A]gencies must often reserve their intervention for the most egregious cases or those which will have the largest impact."[249]

In this digital age, more personal information is susceptible to dispersal and consequently, potential breaches of privacy. Breaches involving names and email addresses should be recognized as harmful themselves because of the emotional, social, and physical suffering.[250] As a proactive endeavor to limit access to users' data, the proposed DNT legislation acknowledges that breaches of users' online privacy are harmful, and aims to create statutory enforcement. Nonetheless, the lack of a private right of action leaves the breach of privacy outside user control to protect or remedy. The legislature may have hoped to avoid frivolous class action lawsuits in the privacy context, but plaintiffs' lawsuits could have been limited to statutorily defined situations where injury exists, such as circumstances of embarrassment, and mental suffering.[251] Furthermore, class action lawsuits can enable a user

246. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. §§ 2(a)(2), 3 (2011). *See generally* 15 U.S.C. § 41 (2006).

247. S. 913 § 3(b)(1), (3)(B).

248. Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 Loy. Consumer L. Rev. 273, 306 (2006).

249. *Id.*

250. *See* Article discussion, *supra* Part II (C)(2).

251. *See* In re Doubleclick Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Plaintiffs, web users, alleged that the defendant's cookies collected information about them, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the internet, and web

to sue on behalf of all similarly-injured users and serve as an effective, "low-cost means" of fulfilling the goals of a statute.[252] If the DNT statutory goals are effective protection of users' informational privacy, then it suggests that injured users should not be at the mercy of government agencies to bring their claims.[253] Within the context of identity theft from a breach of informational privacy, a private right of action would help shift the costs of injury back to the businesses from which the breach resulted.[254] In turn, a private right of action would also help to police businesses that maintain user-information databases by providing the economic incentive of avoiding litigation to employ better security and business practices.[255] This reasoning can be extended to the broader context of informational data privacy, with private rights of actions acting as incentives for better industry self-regulation, and in turn, reduce the risk of all breach of privacy harms.[256]

Enforcement by regulators, rather than through private actions, can provide a predictable, uniform standard that businesses can rely on and consumers will understand. Yet, a private right of action does not create less certainty and clarity if the statute also provides courts with workable definitions as to what constitutes

---

pages or sites visited on the internet, which the plaintiffs considered personal information and not ordinarily expected to be collected by advertisers. *Id.* at 506-07. The court found that plaintiffs adequately plead that defendant's conduct constituted an offense under 18 U.S.C.S. § 2701(a), but because the defendant's affiliated websites were "users" of Internet access under the Electronic Communications Privacy Act (ECPA), and the submissions containing "personal" data made by users to the defendant's affiliated websites were all "intended" for those websites, the websites' authorization was sufficient to except the defendant's access under 18 U.S.C.S. § 2701(c)(2). *Id.* at 524-26.

252. Victor, *supra* note 248.

253. Lawrence Jenab, *Will the Cookies Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. Kan. L. Rev. 641, 669 (2001).

254. Owen Weaver, *A Missed Opportunity To Bolster Consumer Protection In Massachusetts: How Massachusetts Residents Are Still Without A Private Right of Action After The TJX Security Breach*, 43 New Eng. L. Rev. 677, 702 (2009). *See also,* discussion *supra* notes 80, 94-96 and accompanying text.

255. *Id.* at 702-03.

256. *See* discussion, *supra* notes 102-06, 141-47 and accompanying text.

"harm" in the informational data privacy context. However, the DNT Bills are silent on what constitutes an actual harm. Since it is unlikely that the regulatory authorities would be able to monitor and investigate every violation of a breach of privacy, many assaults to users' privacy and personalities[257] may go unpunished. Thus, the DNT legislation may be a step toward enforcing privacy rights online, but it is ineffective for neglecting a private right of action.

B. Unintended Consequences

1. Overly Broad Scope

The DNT Bills are overly broad in scope because of vague terminology and deficient guiding principles. Furthermore, the enactment of a statutorily broad DNT mechanism will cause the unintended consequences of stripping away Internet customization, and altering free content, while inhibiting permissible first party uses of data. The Bills should be more narrowly focused to protect users from defined online threats of privacy.

Both the House and Senate Bills are overly broad because they do not prohibit tracking by data source or type, and consequently, apply not only to third party uses of consumer data, but also to all first party uses. This broad application—regardless of party or use—results from the Bills not defining what "tracking" is, and in turn, not defining to what the DNT mechanism applies. While there may be privacy concerns associated with data aggregation by first parties, the concept of "Do Not Track" was originally conceived as a means to prevent data aggregation across unrelated websites by third party advertisers,[258] because first party uses of data were viewed as generally consistent with user expectations and thus, less likely to cause harm.[259] However, if first party users of data expand their services into other areas beyond their customers' expectations, and they release informational data,

257. Berger, *supra* note 81, at 18.

258. *See* Alissa Cooper, *Do Not Track. No, Seriously.*, CDT BLOG (Nov. 8, 2007), http://cdt.org/blogs/alissa-cooper/do-not-track-no-seriously.

259. FTC GUIDELINES, *supra* note 77, at iii.

privacy harms may result.[260] For instance, while a user might reasonably expect that individual website operators can track them across their own website, many users do not expect or want companies or their affiliates to be able to track what they browse across unrelated websites.[261] Thus, DNT should be narrowly scoped to address the collection and use of passively shared data, across multiple websites, particularly because such collection is often performed by companies that the consumer is unaware of, and those types of uses are more likely to cause harm.[262]

If enacted, Senate Bill 913 and House Bill 654 expressly grant the FTC complete authority to interpret the law and make amendments without legislative guidance.[263] For instance, Senate Bill 913 states that the FTC should consider six factors when implementing the DNT standards: (1) the appropriate scope of covered conduct and persons; (2) technical feasibility and cost associated with the mechanism; (3) existing mechanisms; (4) how to make the public aware of the mechanism; (5) whether and how information could be collected on an anonymous basis so that it is not subject to the rules; and (6) standards by which personal information can be collected and used to provide a service requested by the user even if the user expressed a Do-Not-Track preference.[264] However, the FTC is not mandated to directly incorporate any of these factors; rather, the FTC has sovereignty in crafting DNT rules.

---

260. For instance, Facebook is a social network that is becoming a leader in online targeted advertising, serving as liaison between advertisers and users. *See* discussion *supra* notes 232-40 and accompanying text. Additionally, Google, without notice or consent to its e-mail customers, automatically set them up with an instant Google Buzz network of friends based on their most frequently contacted email addresses and chat exchanges. *See* discussion *supra* notes 98-101 and accompanying text.

261. *See* JOSEPH TUROW, JENNIFER KING, CHRIS JAY HOOFNAGLE, AMY BLEAKLEY, & MICHAEL HENNESSY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 3 (2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00113.pdf.

262. FTC GUIDELINES, *supra* note 77, at 26.

263. For general enforcement provisions, *see* H.R. 654 § 3; S. 913 § 3.

264. S. 913 § 2(c).

The Bills also grant complete deference to the FTC on two other crucial aspects of the DNT mechanism. First, the Bills are silent on standards for monitoring companies' compliance, and procedures for recording compliance or violations, leaving fundamental decisions for discovering privacy violations up to the FTC.[265] Second, the Bills do not firmly define what "personal information" is affected by the legislation. Senate Bill 913 is silent on what constitutes "personal information," and instead, directs the FTC to define the term.[266] Although the House Bill defines "personal information," it also permits the FTC to modify the statutory definition.[267] Thus, the Bills give the FTC unencumbered authority to interpret the law and make amendments without substantial legislative guidance. Congress' lack of guidance is disproportionate to the substantial effect the legislation could have on commerce and privacy rights. Moreover, complete deference to the FTC is not in accord with the Obama Administration and the Commerce Department, whom recommended strengthening FTC enforcement authority, but not allocating all legislative functions to the agency.[268]

a. Free Content

If enacted, the DNT Bills will restrict access to users' information, and likely cause a loss in revenue obtained from targeted advertisements. In turn, this could diminish the amount of free content on the Internet. The loss in revenue may also adversely affect small businesses that tend to rely on advertising revenue for substantial financial support.

Surveys have shown that in general, consumers care about their online privacy and are willing to take steps to protect it,[269] and they

265. For general enforcement provisions, *see* H.R. 654 § 3; S. 913 § 3.

266. S. 913 § 2(a)(1).

267. H.R. 654 § 2(4)(B).

268. Strickling, *supra* note 5. *See also* discussion, *supra* notes 146, 225, and 231, and accompanying text.

269. Harbour, *supra* note 48, at 2-3.

do not like how targeted advertisements are selected.[270] About 66 percent of American adults reject the concept of behaviorally targeted advertisements.[271] When consumers learned about the employed behavioral advertising techniques, over 75 percent rejected the behavioral targeting concept.[272] However, scholars argue that the benefits of behavioral advertising can outweigh the associated risks.[273] One benefit of behavioral advertising is that it generates funding for free content on the Internet.[274] For instance, content providers can pay to provide a service to users, called an advertising-based approach.[275] Under this model, behavioral advertising allows advertisers to target the specific demographic group most likely to be receptive to the advertisement, and increasing its chances of the highest return on investment.[276] Alternatively, users can pay directly for a service, called a subscription-based approach.[277]

A 2010 study from the Network Advertising Initiative (NAI), found that 6.8 percent of people who click on behaviorally targeted advertisements proceed to buying, as opposed to 2.8 percent of online users who click on non-targeted advertisements.[278] Accordingly, "'[t]his study demonstrates the increasing significance of behavioral advertising to the economic model supporting free online content and services for consumers, as well as the need for careful consideration of policies that would affect

---

270. Miguel Helft and 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.

271. Turow, *supra* note 261, at 3.

272. *Id.*

273. Berger, *supra* note 81, at 30.

274. *Id.* (citing Andrew Hotaling, Comment, *Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioral Advertising*, 16 COMMLAW CONSPECTUS 529, 540 (2008), *available at* http://commlaw.cua.edu/res/docs/11_Hotaling.pdf).

275. Berger, *supra* note 81, at 31.

276. *Id.*

277. *Id.* at 30-31 (2011).

278. Caroline McCarthy, *Study: Like It or Not, Behavioral Ad Targeting Works*, CNET NEWS (Mar. 24, 2010), http://news.cnet.com/8301-13577_3-20001069-36.html?tag=mncol;3n.

the current online advertising marketplace and the innovation it supports.'"[279]

With behavioral targeting, consumers view advertisements that are more relevant and useful to their interests, and in turn, revenue resulting from those advertisements can fund free Internet content.[280] For instance, Google funds its free email service, search utility, and map services through revenue from online advertising.[281] Generally, a website operator does not earn money from an advertiser until a user clicks on an advertisement, and this is arguably less likely to happen if the advertisement is not customized for the user.[282] If many users opt out of tracking, websites could lose substantial revenue from the loss of targeted advertisements.[283] Websites could try to recoup revenue losses through "paywalls," or fees to enter a website.[284] One concern is that this solution may result in creating two options for consumers: free website entry in exchange for permission to track, and a paid subscription without tracking.[285] This could result in lower income populations having less online privacy, or else being excluded from information which is currently freely available.[286]

---

279. *Id.*

280. Berger, *supra* note 81, at 32.

281. *Id.* (citing Letter from Alan Davidson, Senior Policy Counsel and Head of U.S. Public Policy at Google Inc., to Jessica Rich, Federal Trade Commission, 2 (Apr. 4, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080404google.pdf).

282. Minda Zetlin, *Is Do Not Track Bad for Small Business?*, INC. (Apr. 27, 2011), http://www.inc.com/articles/201104/is-do-not-track-bad-for-small-business.html.

283. *Id.* Steve DelBianco, executive director of NetChoice, an advocacy group, is concerned that "'Do not Track will run small business of the track.'" *Id.*

284. Comment to *Conversations/Live Q&A: "Do-Not-Track" Legislation: Do We Really Need It?Jeff Jarvis Answers Your Questions*, WASH. POST (May 11, 2011, 2:00 p.m.), http://live.washingtonpost.com/google-do-not-track-bill-0511.html. Jeff Jarvis is currently an associate professor and director of the interactive journalism program at City University of New York's Graduate School of Journalism. *Id.* He is also a published writer, active blogger, editor and media consultant. *Id.*

285. *Id.*

286. *Id.*

The loss of targeted advertisements may also disproportionately affect small businesses, since small businesses are often fully supported by advertising.[287] For example, Rick Jaworski fully supports his family and his online business, JoyofBaking.com, with targeted advertising revenue, and fears that DNT legislation could cause his revenue to be cut in half.[288] Policymakers must balance the risk of harm from privacy breaches and the benefits of targeted advertising.

However, the potential for loss of revenue is not a guaranteed outcome of enacting DNT legislation. FTC Chairman Leibowitz stated that most consumers like receiving targeted advertisements and appreciate free Internet content.[289] Furthermore, giving consumers the option to opt out of tracking does not guarantee that most consumers will.[290] The possible negative effect on free content may be overblown.[291] For instance, the behavioral advertising that the DNT legislation would affect constitutes only four percent of all advertising online.[292] If a website, like Joyofbaking.com, substantially depended on targeted advertisements, the site could ask users to allow tracking before they enter the website.[293]

---

287. Zetlin, *supra* note 282.

288. *Id.* JoyofBaking.com uses data aggregators like Google and ContextWeb. *Id.* The website is compensated when a user clicks on an advertisement, or by how many views are generated from the advertisement. *Id.* Non-targeted, generic advertisements do not pay as much as the targeted advertisements. *Id.*

289. Jon Leibowitz, *FTC Chairman: "Do Not Track" Rules Would Help Web Thrive*, U.S. NEWS &WORLD REP.(Jan. 3, 2011), http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz.

290. *Id.*

291. David Daw, *The State of "Do Not Track" on the Internet*, PCWORLD (Apr. 1, 2011, 1:22), http://www.pcworld.idg.com.au/article/381732/state_do_track_internet/. Jonathan Mayer, of Stanford University Law School's Center for Internet and Society, believes that DNT legislation is blown out of proportion. *Id.*

292. *Id.*

293. *Id.*

Russ Glass, chief executive officer of Bizo, strongly supports government regulation over industry self-regulation.[294] Glass supports his position with the supposition that giving users more control over their data makes his company more appealing, because "cultivating trust" is important to a brand's value.[295] In his business, Glass has emphasized transparency, allowing users on Bizo's website to view or edit collected information, or opt out of tracking.[296] Furthermore, Glass is not concerned because users in favor of an opt-out policy usually will not affect revenue, since "users who opt out 'wouldn't have converted [to sales] anyways.'"[297]

If enacted, the DNT Bills will likely cause a decrease in revenue from behavioral advertising, and negatively impact businesses that substantially rely on that form of revenue. However, the exact amount of revenue loss is undeterminable because it depends on user action. This potential loss of revenue will likely also adversely affect the availability of free content on the Internet.

b. Customization

If enacted, the DNT Bills will restrict access to users' information, and likely cause a loss of customization on the Internet, because website operators will not know their customers' preferences in order to customize their Internet experience. For instance, Netflix, an online movie-rental company, suggests other movies for customers based on past selections.[298] Facebook also uses this technology to customize their customers' experiences.[299]

294. Steve Cooper, *Online Tracking Business Bizo Backs "Do Not Track Online" Rules*, BLOOMBERG.COM (May 13, 2011), http://www.bloomberg.com/news/2011-05-13/online-tracking-business-bizo-backs-do-not-track-online-rules.html. Bizo is an online marketing firm that aggregates and sells data on 85 million business professionals. *Id.* Bizo's network uses cookie-technology to create anonymous user profiles based on demographic data from about 1200 sources. *Id.*

295. *Id.*

296. *Id.*

297. *Id.*

298. Berger, *supra* note 81, at 32.

299. *Id.*

Facebook explains that as a first party user of data, uses collected information "as part of our efforts to keep Facebook safe and secure."[300] Facebook uses cookies to make the site easier to use, through such uses as storing login information and protecting the company itself from "malicious activity."[301] Although a user can remove or block cookies through browser settings, Facebook warns that doing so may negatively impact the user's ability to use the website.[302] Customized benefits are arguably enjoyed by users, even if they are not recognized for what they are. However, customized benefits also carry inherent risks.[303] For example, in order to make user recommendations, Facebook stores personally identifying information about its users, so there are risks of identity theft and sensitive data leaks.[304]

Financial company websites often use cookies to recognize registered customers. In its online Security Center, Chase Bank acknowledges that it uses cookies to authenticate a customer and the computer accessing the website.[305] Chase describes how some browsers will allow consumers to disable cookies, but warns that some website features require cookies in order to interact with the user.[306] In particular, Chase uses cookies to store information about customers' machines to enable quick authentication on subsequent visits.[307] If a customer disables cookies on her browser, she will be faced with the inconvenience of fulfilling multiple safeguards protections prior to logging on to her account

300. *Information We Receive and How It Is Used*, *supra* note 232.

301. *Trouble Using Facebook, Cookies*, FACEBOOK.COM, https://www.facebook.com/help/?faq=115180708570932&ref_query=coo (last visited Oct. 26, 2011).

302. *Id.*

303. Berger, *supra* note 81, at 32.

304. *Id.* at 33. Furthermore, Facebook states that they do not use cookies to create a profile of browsing behavior on third-party websites, although they may use anonymous, aggregated data to improve advertisements. *Trouble Using Facebook, supra* note 301.

305. *How We Protect You, Security Center Home*, CHASE, https://www.chase.com (last visited Aug. 22, 2011) (follow "Security" hyperlink).

306. *Id.*

307. *Id.*

on the secure website.[308] If the DNT legislation is enacted, and users implement the broad-spectrum DNT mechanisms, users will be faced with lengthy login procedures on all websites requiring accounts, such as online pharmacies, retail websites, or financial websites. Websites will no longer remember users, identities, or passwords. Inconvenience could translate into diminished commerce on the Internet, as users grow frustrated with the tiresomeness of repeated login procedures. If consumers want to eliminate these inconveniences, resuming the customization of their frequented online services, their only alternative may be to turn off the opt-out tool, leaving themselves vulnerable to tracking across all websites.

The risks associated with behavioral advertising often result from the mishandling of user data, or unforeseen third party security breaches.[309] If these risks can be mitigated, then the benefits to users and profilers are mutually shared.[310] Thus, it can be argued that in general, this technology is viewed as more helpful than harmful.[311] Since the risk of harm to users is low, it does not make sense to impede the advancement of tracking technology.[312] If users enable a universal DNT opt-out tool, users may find their Internet experience would not include many of the perks and personalization they are used to experiencing. This could result in an overall diminished online experience.

2. Technical Implementation & Flexible Control

Although the Bills propose a browser-based DNT mechanism to allow users to universally opt out of all data collection across the Internet,[313] browser-software companies have implemented

308. *Id.*

309. *See* Article discussion, *supra* Part II (D).

310. Berger, *supra* note 81, at 30.

311. *Id.*

312. *Id.* at 32 (citing Bennet Kelley, *Privacy and Online Behavioral Advertising*, 11 J. OF INTERNET L. 24 (2007) (indicating that during FTC hearings, advocates of stricter regulation failed to demonstrate specific cases of harm)).

313. Do-Not-Track Me Online Act of 2011, S. 913, 112th Cong. § 2(a)(1)-(2) (2011).

browser tools that allow users to voluntarily opt out of being tracked across the Internet. These browser-based opt-out tools provide a baseline, universal protection already available to users. However, the Bills are silent on the mechanics and flexibility of their proposed DNT tools.

Even though the FTC has not previously endorsed a particular DNT mechanism,[314] the FTC Commissioner defined the elements a comprehensive DNT mechanism should embody, to allow consumers the choice to opt out of having their online activity followed, recorded, collected, and shared.[315] To be effective, a DNT mechanism should apply to all websites universally. The mechanism should be easy to find, understand, and use.[316] Furthermore, users' preferences should be persistent through clearing cookies or updating browser programs.[317] The opt-out preference should comprehensively apply to collection of all online data, for any purpose other than product or service fulfillment.[318] It should be effective and enforceable without technical loopholes.[319] Finally, the preference to opt out should apply to collection of online data for any purpose other than product or service fulfillment.[320] The FTC also advises that a DNT tool should be flexible, and allow for companies to try convincing consumers not to opt out of tracking by explaining the benefits of tracking and behavioral advertising.[321]

If the DNT legislation is enacted, maintaining flexibility for users will be a key design element. For instance, a user may want to allow tracking on reputable websites she feels provide value in exchange for the tracking data, but she may want to disable tracking on unfamiliar websites.[322] Although the FTC has

314. Joelle Tessler, *"Do Not Track" Challenges Tech Industry*, USATODAY (July 26, 2011), http://www.usatoday.com/tech/news/2011-07-26-mozilla-chrome-internet-explorer-privacy_n.htm.

315. Brill, *supra* note 4, at *6.

316. *Id.*

317. *Id.*

318. *Id.*

319. *Id.*

320. *Id.*

321. Brill, *supra* note 4, at *6.

322. Daw, *supra* note 291.

endorsed the concept of flexibility for DNT tools, this concept is not mandated in the proposed legislation, and the FTC is not bound to implement the concept.

Microsoft has instituted a feature called "tracking protection" in Internet Explorer 9.0 that lets users separate "black lists" of blocked websites, and "white lists" of accepted websites.[323] Microsoft's solution requires users to determine what websites require blocking, and vigilant user intervention on a site-by-site basis.[324] While this program gives users freedom in what websites they restrict, this can also be detrimental because users must determine what websites should be blocked.[325] Since tracking is generally not a visible process,[326] this may be very difficult for users to implement. To try to combat this hurdle, Internet Explorer 9.0 can automatically build blocked and allowed lists of websites, or users can download existing lists.[327] Yet, canned lists may not be suitably tailored for each user, depending on his or her Internet activity. Moreover, automatically-built lists may block websites that the user does not want blocked, and therefore, still require intense user involvement to manage the lists.

Mozilla also has a new privacy feature that allows users to enable a DNT setting in their browser's header, which sends a signal to alert website advertisers that the user has opted out of tracking.[328] Mozilla's solution is easier to use than Microsoft's because it requires less user involvement and is more stable than a cookie-based solution.[329] However, one problem with the solution is that it relies on websites to look for the DNT header.[330] Another

323. Tessler, *supra* note 314.

324. Tony Bradley, *Firefox Do-Not-Track Feature Has a Fatal Flaw*, PCWORLD (Jan. 24, 2011, 5:41 AM), http://www.pcworld.com/businesscenter/article/217478/firefox_donottrack_feature_has_a_fatal_flaw.html.

325. *Id.* The author opines that Internet Explorer 9 will require "too much" user intervention. *Id.*

326. *See* Article discussion, *supra* Part II (B).

327. Tessler, *supra* note 314.

328. *Id.*

329. Bradley, *Firefox*, *supra* note 324.

330. Tony Bradley, *Why Browser "Do Not Track" Features Won't Work*, PCWORLD (Feb. 10, 2011), http://www.pcworld.com/businesscenter/article/219328/why_browser_do_not_track_features_wont_work.html.

problem is that unless websites honor the opt-out preference, there is nothing to technologically prevent websites from tracking.[331] Furthermore, the Bills are silent on methods of non-compliance detection, monitoring, and recording violations.[332] Consequently, it is unclear how reliance on companies' good faith respect of users' preferences will be alleviated by the passing of the DNT legislation. Although more effective than Microsoft's cookie-solution, Mozilla does not solve the problem with "sites that cross the line and abuse tracking, [that] already know that their activities are ethically wrong and frowned upon by both the FTC and the general public."[333] Yet, Mozilla's solution is "technically elegant," and will likely influence further privacy innovation.[334]

Google's Chrome browser is offering an add-on feature that maintains opt-out cookies even if other types of cookies are deleted, and solves the problem of users losing their opt-out preferences when they clear their browser cookies.[335] Google's solution requires users to know about the add-on.[336] As with Mozilla's solution, this add-on's effectiveness at preventing tracking relies heavily on the self-regulation efforts of the advertising companies conducting the tracking.[337] For a DNT tool to work, there must be a consensus on what constitutes tracking.[338]

If DNT legislation is enacted, implementing the DNT mechanisms will be more complicated in practice than simply adding IP addresses to a database. One challenge is in reaching an industry consensus on the definition of DNT obligations, when

---

331. Bradley, *Firefox, supra* note 324.

332. For general enforcement provisions, *see* Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. § 3 (2011); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. § 3 (2011).

333. Bradley, *Firefox, supra* note 324.

334. Bradley, *Why Browser "Do Not Track" Features Won't Work*, *supra* note 330. Bradley quotes an email send to him by an Electronic Frontier Foundation (EFF) spokesperson, endorsing the DNT approach as a "major step in the right direction."

335. Tessler, *supra* note 314.

336. Bradley, *Why Browser "Do Not Track" Features Won't Work*, *supra* note 330.

337. *Id.*

338. Tessler, *supra* note 314.

even the FTC itself has a malleable definition of tracking.[339] For instance, websites could be allowed to measure traffic volumes on their own websites, but should advertisers also be allowed to track how many visitors see or click-through on their advertisements?[340] Furthermore, privacy advocates are dissatisfied that the advertising industry's self-regulatory guidelines do not mandate turning off data collection.[341] Instead, users who install an opt-out cookie no longer receive targeted advertisements from participating companies but can still be tracked for non-advertising purposes, such as data cataloging and resale.[342] However, the FTC's recommendation of a flexible standard does not seem to be accounted for in the proposed legislation, as the Bills call for a universal opt-out mechanism. The FTC recognized that some targeting is acceptable, and companies should be allowed the opportunity to convince users of its benefits.[343] If DNT is enforced too broadly—as a blanket DNT browser tool—companies may be shut out before the user finishes opening up the browser program. If DNT legislation is enacted, a user's opt-out preference would apply universally, regardless of the website's intent for collecting data. The only exceptions to this rule would be for the collection of data to process user-initiated transactions, and for accomplishing currently accepted business practices, such as billing.[344] The proposed DNT legislation does not mandate flexibility or control within the DNT mechanism, which would enable the user to personalize control and allow tracking for selected websites. This, in turn, does not empower the user to control their susceptibility to online tracking; rather, the DNT Bills potentially leave users with an absolute choice of being invisible on the Internet, or being vulnerable.

If DNT legislation is enacted, the implementation of a standardized DNT tool must balance simplification for all types of

339. *Id.* *See also*, Bob Liodice, President and CEO of Assoc. of Nat'l Advertisers (ANA), Liodice Statement on Proposed DNT Legislation (March 9, 2011), http://www.iab.net/public_policy/1617651.

340. Tessler, *supra* note 314.

341. *Id.*

342. *Id.*

343. Brill, *supra* note 4, at *6.

344. For general exemptions, *see* H.R. 654 § 3(d)(1)-(7); S. 913 § 2(b).

users, with sophistication for the needs of all types of websites. To be effective, a DNT mechanism should be easy for a user to find, understand, and use.[345] Furthermore, the implementation must also balance granting consumers the ability to stop tracking technology for marketing purposes without preventing tracking critical to functionality.[346] For example, Internet companies rely on tracking not just to target advertisements, but also to store user's passwords and login preferences, and to deliver user-customized content, such as local news.[347] The texts of the DNT Bills do not make a distinction between tracking for different purposes. Instead, it would solely be up to the FTC to promulgate rules that would separate out intent.

The DNT legislation also faces the challenge of implementing a DNT mechanism to regulate rapidly changing technology. Many technology-based laws are outdated before they are fully implemented because of the time it takes to put a law into operation.[348] In this respect, industry self-regulation may be better equipped to adapt to the changing needs of technology and business-specific industries.[349] Due to the lack of legislative guidance for a flexible DNT mechanism, the DNT Bills render implementation virtually boundless, within the exclusive power of the FTC, and entirely problematic.

V. CONCLUSION

Online tracking and personal privacy are not necessarily incompatible, but finding a balance between informational privacy rights and preserving customized features of the Internet has created a delicate problem for advertising companies, commercial programmers, and regulatory authorities. Currently, there is no federal statute preventing websites from disregarding users'

345. Brill, *supra* note 4, at *6.

346. Tessler, *supra* note 314. Marc Rotenberg is the executive director of the Electronic Privacy Information Center and warns about the dangers associated with DNT mechanism. *Id.*

347. *Id.*

348. Zetlin, *supra* note 282.

349. *Id.*

decisions to opt out of tracking.[350] Some users may have no idea that tracking and collection of personal information occurs online, while others are troubled by the surveillance. Still others may be aware that data collection occurs, but view it as a necessary trade-off for taking advantage of the online services and content. One survey indicated that 85 percent of consumers want the ability to control whether or not they are tracked online,[351] but this does not necessarily correlate into good public policy. Those in opposition to the DNT legislation point out that many online users already have opt-out capabilities through browser settings. However, users do not have recourse if websites track their use, regardless of their browser settings. While current DNT legislation aims to regulate rogue websites that ignore users' opt-out preferences, enforcement would remain only in the hands of the government.

The FTC supports a universal DNT mechanism that does not stifle technological innovation and preserves users' control over their informational data.[352] In response, Michael Zaneis, senior vice president and general counsel of the Interactive Advertising Bureau, opines that the self-regulated advertising industry is more capable of enforcing promises of privacy protection.[353] To illustrate, Zaneis offers, "[t]hink about the diminished consumer experience that heavy-handed regulation could cause and contrast it to the positive experience you get when you add yourself to the Do Not Call list.[354] Think about that the next time you check the sports scores on your smartphone."[355]

350. Daw, *supra* note 291.

351. Leibowitz, *supra* note 289.

352. *Id.*

353. Michael Zaneis, *"Do Not Track" Rules Would Put a Stop to the Internet as We Know It*, U.S. NEWS & WORLD REP. (Jan. 3, 2011), http://www.usnews.com/opinion/articles/2011/01/03/do-not-track-rules-would-put-a-stop-to-the-internet-as-we-know-it.

354. *Id.; see* https://www.donotcall.gov/. The National Do Not Call Registry allows consumers to opt out of receiving telemarketing calls on home or mobile phones. *Id.* If telemarketers call a registered number, a consumer can file a complaint at the aforementioned website. *Id.*

355. Zaneis, *supra* note 353.

In a 2010 survey, Internet users sent somewhat conflicting messages about the influence of targeted advertisements.[356] For instance, more than six in ten users have noticed advertisements targeted to them based on their browsing history, but nine in ten users said that they generally ignore online advertisements.[357] While the data summarizing consumers' opinions of targeting advertising is somewhat unclear, what is certain is consumers' desire to maintain control over their own privacy. [358] However, the DNT legislation appears to be an ineffective solution to protecting users' informational privacy. Users are not fully empowered by the Bills because they do not provide a private right of action. If enacted, the overly broad DNT Acts would enable a blanket opt-out tool, depriving consumers of some beneficial tracking, such as tracking performed to prevent fraud, or monitor unauthorized use of financial information, such as in identify theft situations.[359] Also, tracking users online can avoid sending users the same advertising repeatedly.[360] Tracking users can allow companies to compile data as user feedback, and facilitate conducting analytics that foster technical innovation.[361] Furthermore, the DNT mechanism will strip away Internet customization, and alter free content. Finally, a technical loophole could leave users vulnerable on social networking websites, which have become a leading forum for Internet advertising.

What is remarkable about the DNT legislation is the role-reversing effect it has had on the U.S. stance in the worldwide privacy debate. The European Union, historically a trailblazer for individual privacy rights, is now following the United States' lead

356. Lyman Morales, *U.S. Internet Users Ready to Limit Online Tracking for Ads*, GALLUP (Dec. 21, 2010), http://www.gallup.com/poll/145337/internet-users-ready-limit-onlinetracking-ads.aspx.

357. *Id.*

358. *Id.* The article discusses the results from a USA TODAY/Gallup poll conducted on December 10-12, 2010. *Id.*

359. Thomas Rosch, *The Dissent: Why One FTC Commissioner Thinks Do Not Track is Off-Track*, ADVERTISING AGE (Mar. 24, 2011), *available at* http://adage.com/article/guest-columnists/ftc-commissioner-thinks-track-track/149558/.

360. *Id.*

361. *Id.*

in adopting DNT legislation.[362] Neelie Kroes, the European Commissioner for the Digital Agenda, called for the E.U. to adopt "do not track" legislation similar to the proposed Bills:

> I think we should collectively pay more attention to the emerging "do-not-track" technologies . . . DNT is already deployed in some web browsers. And some web businesses say they honor it. But this is not enough. Citizens need to be sure what exactly companies commit to if they say they honor DNT. For example, there is an important difference between a commitment not to record tracks and a commitment not to use them for a specific purpose once recorded. When this is solved more users will deploy DNT—and it will become simpler—and companies will go along ... How do we get there? We need a standard![363]

The proposed DNT Bills have made an impression on the online advertising industry, the regulatory authorities, and world leaders in privacy initiatives. Although the Bills do not fully resolve current issues for online data privacy, the y have succeeded in underscoring online users' concerns and awakening bipartisan dialogue. Legislators have attempted to strike a balance between protecting online privacy, and preserving online content. However, the issue is not just about data being tracked; it is the limitless retention of user data and what is done with that data once it has been obtained. Perhaps an alternative approach would be to regulate what companies are allowed to do with user data, rather than trying to prevent companies from obtaining user data. For instance, if data were collected about a user due to user error, such as the user accidentally deactivating the browser opt-out

362. Sharon Fischer, *European Union Calls for 'Do Not Track' Legislation Like the U.S. is Working On*, CMSWIRE (June 23, 2011), http://www.cmswire.com/cms/web-engagement/european-union-calls-for-do-not-track-legislation-like-the-us-is-working-on-011787.php.

363. *Id.*

feature, the proposed DNT legislation does not offer the user any protection. In combination with industry self-regulation, statutory data-retention limits would protect users' data by default, and in turn, their privacy.

*Stephanie A. Kuhlmann**

---

* J.D. Candidate 2013, DePaul University College of Law; M.A. 2004, Syracuse University; B.A. 2002, Vanderbilt University. I would like to thank Professor Martin Robins for his valuable guidance and feedback.