How Internet Users' Identities Are Being Tracked and Used

Alexandra Drury*

I. INTRODUCTION

In the past decade, the Internet has grown exponentially. In 2010, the average American spent thirty-two hours a month on the Internet.[1] Some might think that number is high, but Americans and others around the world are increasingly living their lives "online." Whether Internet users are online chatting on Facebook with old friends, searching Google for the perfect present, or participating in online forums, the Internet is now, more than ever before, being used for almost every aspect of people's lives. While most Internet users recognize its benefits, many do not stop and think about its costs. Internet users believe that they are

* © 2012 Alexandra Drury. J.D. candidate 2013, Tulane University Law School; B.A. International Relations 2009, University of California Davis. The author would like to thank her family for all of their support and guidance and the members of the *Tulane Journal of Technology and Intellectual Property* for all of their hard work.

1. *Average Time Spent Online per U.S. Visitor in 2010*, COMSCORE DATA MINE (Jan. 13, 2011), http://www.comscoredatamine.com/2011/01/average-time-spent-online-per-u-s-visitor-in-2010/.

going about their business on the Internet fairly unnoticed, but that simply is not the case. This Comment will explore how the trust that many Internet users have in the Internet is misguided due to the lack of privacy inherent in Internet use.

Part II will reveal the various ways an Internet user can be tracked, specifically the process of "scraping" data from Web sites. The way in which some Web sites sell the user's information for advertising purposes will also be examined. The last way an Internet user can be tracked is through the use of "zombie cookies"—respawning cookies that are placed on a user's hard drive so that a Web site can track a user's every online movement.

Part III will look at the manner in which Web sites utilize a user's information after they employ any of the above-mentioned methods of gathering said information. Here, the diverging views on the benefits of Internet tracking will be analyzed. On the one hand, Internet companies claim that the collection of user data benefits users by providing them with safety and protection. Proponents also assert that scraping provides a greater overall benefit to the economy as a whole. On the other hand, many Internet users, bloggers, and politicians argue that Internet companies are gathering this information for their own financial gain.

Parts IV and V will examine—via the judiciary and legislature—the issue of tracking and using Internet users' personal information. Part IV of this Comment will analyze the manner in which courts are presently dealing with the issue of online privacy. Part V will examine a newly proposed online privacy bill by reviewing the bill's various provisions and discussing critics' current reaction.

Finally, the Comment will conclude with the author's thoughts on where online privacy needs to go from here in order to ensure that Internet users are well-protected without stifling Internet growth and with suggestions as to how Internet users can currently protect their online privacy.

II. HOW INTERNET USERS ARE BEING TRACKED

A. Scraping

As Web sites and companies have expanded the way in which individuals are able to utilize the Internet, both entities have also been looking for ways to use the individuals on the Internet for their own benefit. One of the methods employed is the process of "scraping,"

which entails "copying" Internet users' personal information.[2] Scraping occurs through firms which offer to gather Internet users' online conversations to collect detailed information about them.[3] Scrapers gain information from places such as job sites, social networking sites, and even online forums and message boards where people reveal personal and intimate details about their lives.[4] As some Web sites try to protect their users, scrapers attempt to outsmart the Web sites' defenses.[5] One way scrapers try to do this is by staging multiple, simultaneous attacks on a single Web site in order to break through the Web site's defenses—if only for a short period of time—in order to "grab as much data as quickly as possible without being detected or crashing the site they're targeting."[6] Scrapers then compile this information and sell it to any number of companies or organizations.[7] Often, scrapers are also hired by clients to take specific information from a Web site.[8]

So what do these companies that hire scrapers do with an Internet user's personal information? Some companies use scraping as a means to collect personal information for background reports that can include individuals' cell phone numbers, photographs, e-mail addresses, and even posts to social networking sites.[9] Some employers hire scrapers to find out information about prospective employees.[10] People can even do a "Date Check" for $14.95, which gives them the personal information of a potential date.[11]

Internet users' personal information can also be gathered from public records and online profiles, making one large database of a person's information.[12] Take the Web site Spokeo for example: just by typing in a person's first and last name, a user can obtain information

---

2. *See* Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, WALL ST. J. (Oct. 11, 2010, 9:30 PM), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html.

3. *See id.*

4. *See id.*

5. *See id.*

6. *Id.*

7. *See id.*

8. *Id.*

9. *See id.*

10. *See id.* In one instance, a large insurance company also used scraping to find names of agents that were working for competitors. *See id.*

11. *See id.* This same site, Intelius, offers other services such as criminal background checks. *See id.* Another Web site, PeekYou LLC, has discovered a way to match users' "real names to the pseudonyms they use on blogs, Twitter, and other social networks." *Id.* As of October 2010, PeekYou LLC had records of "about 250 million people, primarily in the U.S. and Canada." *Id.*

12. *See id.*

such as a person's age, occupation, place of residence, home value, marital status, interests, ethnicity, and many other details about the person's life.[13] The site also offers more information if a user wants to pay a fee as small as $2.95 a month.[14] If a user does want to become a member of the site, they can obtain additional information such as a person's phone number, names of relatives, and e-mail address.[15] While some of the information Spokeo reveals is public record, most people would not go out of their way to find out all of these details about another person's life on their own. But when the hurdle to discovering that information is only a few keystrokes, people are more inclined to discover whatever detailed personal information they can about another person.

B. Web Sites Compiling Users' Data

While scraping is one method used by third parties to gather Internet users' personal information, another is employed by the Web sites that a user visits.[16] Many users are not aware that Web sites they use routinely send their personal information to other companies.[17] Simply visiting a local ad on the Home Depot Web site will send the user's first name and e-mail address to thirteen companies.[18] Likewise, interacting with the Web site Classmates sends a user's first and last names to twenty-two companies.[19] Even more startling is how Metacafe sends two companies a user's first and last names, e-mail address, physical address, birthday, and phone number when that user changes his or her user settings.[20] Other more personal information—such as a member's smoking, drinking and drug use habits, his ethnicity, and income[21]—can be sold to companies by Web sites for which a member actually signs up.[22]

---

13. *See* SPOKEO, http://www.spokeo.com/ (last visited Oct. 3, 2012). The Web sites PeekAnalytics and RapLeaf also compile and scrape Internet users' personal information for others' use. *See* PEEKANALYTICS, http://peekanalytics.com/ (last visited Oct. 3, 2012); RAPLEAF, https://www.rapleaf.com/ (last visited Oct. 3, 2012).

14. *See* SPOKEO, *supra* note 13.

15. *See id.*

16. *See* Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, CENTER FOR INTERNET & SOC'Y, STAN. L. SCH. (Oct. 11, 2011, 8:06 AM), http://cyberlaw.stanford.edu/node/6740.

17. *See id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *See id.*

22. *See id.* For example, it seems that the online dating Web site OkCupid sells its members profile information to BlueKai and Lotame, both of whom are data providers. *See id.*

What is more disconcerting is that Web sites often break their promises of user anonymity by disseminating purportedly private information.[23] Companies that purchase a user's information more than once are able to decipher a user's online pseudonym and identify the real person.[24] Once a user is identified, it not only affects future tracking of the user, but also retroactively affects the user's data that has previously been collected.[25] So even if a Web site discloses that it gives its users' information to companies anonymously, there is a significant chance that users' personal information will be linked back to them by name.

While users might believe what Web sites tell them—that simply deleting their information or cookies[26] that are placed on their hard drives will protect their information—they are often wrong. Even when users pay a company to delete their information, it may be only a temporary solution.[27] Issues with tracking, continuing after users think they have taken the appropriate steps to combat it, have been rampant with some of the Internet's largest companies.[28] Such continued tracking can be accomplished by using devices commonly known as "zombie cookies."[29] Even amidst numerous lawsuits regarding the use of "zombie cookies," companies such as Microsoft continue to employ them.[30] When a user finds the cookie and deletes, disables, or blocks it, so they are no longer tracked, the cookie simply recreates itself and continues tracking.[31]

---

23. *See id.*

24. *See id.*

25. *Id.*

26. These cookies are embedded in Internet users' hard drives when they visit any number of sites.

27. *See* Julia Angwin, *Sites Are Accused of Privacy Failings*, WALL ST. J. (Feb. 13, 2012), http://online.wsj.com/article/SB10001424052970204136404577207183258570186.html. Reputation.com, a service that deletes personal data for a price, reported that about ten percent of records they had removed reappear every day. *Id.*

28. *See* Woody Leonhard, *'Zombie Cookies' Won't Die: Microsoft Admits Use, HTML5 Looms as a New Vector*, INFOWORLD (Aug. 22, 2011), http://www.infoworld.com/t/internet-privacy/zombie-cookies-wont-die-microsoft-admits-use-and-html5-looms-new-vector-170511. Cookies are commonly attached to a user's hard drive for harmless things such as passwords and user IDs, but many others are used for marketing purposes. *See* Stanton McCandlish, *EFF's Top 12 Ways To Protect Your Online Privacy*, ELECTRONIC FRONTIER FOUND. (Apr. 10, 2002), http://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy. A company can among other things track a user's motions through a Web site, the amount of time spent there, and what other links were clicked. *See id.*

29. Leonard, *supra* note 28.

30. *See id.* MySpace, NBC Universal, Disney, and Hulu are among the companies that have been sued over their use of zombie cookies. *See id.*

31. *See id.* For example, Microsoft was embedding these cookies whenever an Internet user visited MSN.com, Microsoft's U.S. homepage, or the Microsoft Store. *Id.*

III. HOW WEB SITES ARE USING IDENTIFYING INFORMATION

A. For the Users' Benefit?

Now that it is clear that Internet users' online and real personalities are being tracked, the question remains: why are they being tracked? Some Web site employees claim that it is for the users' benefit.[32] For example, a Facebook engineer commented on an Internet post that its logged-out cookies are for its customers' own "safety and protection."[33] The engineer went on to explain how the cookies that track members even after they are logged out—the ones that so many Internet users and commentators are upset about—are used specifically to help Facebook's members.[34] Among the ways these cookies are used for the members' online security and protection are:

> identifying spammers and phishers, detecting when somebody unauthorized is trying to access your account, helping you get back into your account if you get hacked, disabling registration for a [sic] under-age users who try to re-register with a different birthdate, powering account security features such as 2nd factor login approvals and notification, and identifying shared computers to discourage the use of 'keep me logged in.'[35]

The Facebook engineer stated that cookies that are used while members are logged in to their Facebook accounts are also used for members' benefit.[36] These cookies are used to personalize a member's Facebook page and help Facebook maintain and improve user experience.[37]

Google expressed some of the same sentiment as the Facebook engineer above. With so much backlash aimed at Google's new privacy policy, the company explained that its use of members' information

---

32. *See* Graeme McMillan, *Facebook Cookies Work Even If You're Logged Out (for Your Own Good)*, TECHLAND, TIME (Sept. 26, 2011), http://techland.time.com/2011/09/26/facebook-cookies-work-ven-if-youre-logged-out-for-your-own-good/ (citation omitted).

33. *Id.* The comment was in response to an article in which hacker Nik Cubrilovic claimed that Facebook was using cookies to track its members even when they were logged out. *See id.* Emil Protalinski, the article's author, seemed to purport that the company was using these cookies for reasons that are inconsistent with what members and potentially governments (such as Germany) want, stating, "[T]his could be a serious problem for Facebook." Emil Protalinski, *Facebook Tracks You Online Even After You Log Out*, ZDNET (Sept. 25, 2011, 7:59 AM PDT), http://www.zdnet.com/blog/facebook/facebook-tracks-you-online-even-after-you-log-out/4034?tag=content;siu-ontainer.

34. *See* McMillan, *supra* note 32.

35. *Id.* (citation omitted).

36. *Id.*

37. *See id.*

benefits users.[38] On Google's Public Policy blog, the company stated that its new privacy policy utilizes users' data to "refine and improve [users'] experience."[39] In combining more than sixty product-specific privacy policies, Google stressed that it is not doing so to intrude on its users' privacy, but rather to create one short, easy-to-understand policy combining user data to make each user's experience simpler and more personalized.[40] Combining all of its often-used services such as Gmail, YouTube, Calendar, and Search, Google can better understand and help facilitate successful searches for its members as well as ease users' mobility across Google's various services.[41] For example, Google explained that its new policies allow users that are signed-in to directly "add an appointment to their Calendar when a message in Gmail looks like it's about a meeting, or read Google Docs within their email."[42] Although Google claimed that its new policy is for the benefit of its users, the company also sought to assure users that they could still protect and control their personal information, which would not be sold, rented, or traded to third parties.[43]

Along with Facebook and Google, scrapers assert similar benefits arising from the collection of private data. For instance, targeted advertising is a product of data analysis from scraping. It benefits users, because targeted advertising exposes users to advertisements that might actually interest them.[44] Proponents of scraping bolster their argument by stating that scraping benefits "a rapidly expanding data economy," of

---

38. *See Q&A: Google's Controversial New Privacy Policy*, CBS NEWS (Feb. 29, 2012, 11:47 PM), http://www.cbsnews.com/8301-205_162-57388186/q-a-googles-controversial-new-privacy-policy/; *see also U.S. Regulators Probe Google's Privacy Issues*, NPR (Mar. 16, 2012), http://www.npr.org/2012/03/16/148732683/business-news; Betsy Masiello, *Setting the Record Straight About Our Privacy Policy Changes*, GOOGLE PUB. POL'Y BLOG (Jan. 26, 2012, 5:54 PM), http://googlepublicpolicy.blogspot.com/2012/01/setting-record-straight-about-our.html.

39. Masiello, *supra* note 38.

40. Pablo Chavez, *Changing Our Privacy Policies, Not Our Privacy Controls*, GOOGLE PUB. POL'Y BLOG (Jan. 31, 2012, 7:59 AM), http://googlepublicpolicy.blogspot.com/2012/01/changing-our-privacy-policies-not-our.html. Google states that its new privacy policy will have eight-five percent fewer words. *Id.*

41. *Policies and Principles*, GOOGLE, http://www.google.com/policies/ (last visited Oct. 20, 2012). By tracking a user's history, Google explains that it can better understand what a user means when she searches for the words "Pink" or "Jaguar" and help obtain more targeted results. *Id.*

42. Betsy Masiello, *Busting Myths About Our Approach to Privacy*, GOOGLE PUB. POL'Y BLOG (Feb. 1, 2012 2:13PM), http://googlepublicpolicy.blogspot.com/2012/02/busting-myths-about-our-approach-to.html.

43. *See id.*

44. *See* Jonathan Leger, *The Advantages of Internet Marketing in a Bad Economy*, JONATHAN LEGER—SEO AND INTERNET MARKETING BLOG (Oct. 15, 2008), http://www.jonathanleger.com/the-advantages-of-internet-marketing-in-a-bad-economy/.

which Internet users are all a part.[45] In 2009 alone, marketers spent $410 million on online data, and that number should double to $840 million in 2012.[46]

B. For Web Sites' Benefit?

Unfortunately for online giants like Google and Facebook, users, bloggers, and some government officials do not agree that the way in which companies track consumers and utilize their data is primarily altruistic. For one, Bilal Ahmed does not believe that scraping is beneficial to him.[47] Mr. Ahmed, a thirty-three-year-old man suffering from depression, used the Web site PatientsLikeMe to talk on the site's private online forums about very personal information relating to his depression.[48] Along with personal stories about his depression, the site also contained a list of drugs that he used.[49] In 2010, the site was scraped, copying every single message Mr. Ahmed had ever written on these private forums, where he had once felt safe to talk about his health issue.[50] Mr. Ahmed stated that when he found out that the site had been scraped and his information copied in order to be sold, he "felt totally violated."[51] Not only had Mr. Ahmed's medical information been copied, which is disturbing in and of itself, but because his blog was linked to his pseudonym on the Web site, companies could easily find out exactly who he was.[52] A very disconcerting aspect of scraping is that, as one owner of a scraping company has indicated, they turn a blind eye to whether or not the person paying his company to scrape is using the information for illegal purposes.[53]

Likewise, Nick Bergus certainly would not believe that Facebook's use of his information and tracking of what he did online was for his benefit.[54] Via another Web site, Mr. Bergus' attention was directed to an item for sale on the Web site Amazon that he found comical.[55] This item was a fifty-five-gallon drum of Passion Natural water-based lubricant

---

45. *See* Angwin & Stecklow, *supra* note 2.
46. *Id.*
47. *See id.*
48. *See id.*
49. *See id.*
50. *See id.*
51. *Id.*
52. *See id.*
53. *See id.*
54. *See* Nick Bergus, *How I Became Amazon's Pitchman for a 55-Gallon Drum of Personal Lubricant on Facebook*, NICK BERGUS (Feb. 23, 2012), http://nbergus.com/2012/02/how-i-became-amazons-pitchman-for-a-55-gallon-drum-of-personal-lubricant-on-facebook/.
55. *Id.*

that cost $1,495.[56] Finding it amusing, Mr. Bergus posted the link to Facebook on February 14, 2011, with a line attached that read: "A 55-gallon drum of lube on Amazon. For Valentine's Day. And every day. For the rest of your life."[57] A week later, Mr. Bergus was contacted by people he knew saying that his post about the lubricant was regularly showing up next to friends' news feeds as a "sponsored story."[58] The post was showing up on so many of Mr. Bergus's friends' pages so frequently because Amazon was paying Facebook to highlight that link for advertisement purposes.[59] Most of Facebook's revenue comes from advertisements,[60] and Facebook's CEO Mark Zuckerberg has recognized that when it comes to advertising, people are highly influenced by recommendations from people they trust, such as their friends.[61] Facebook has turned its users, like Mr. Bergus, into its own personal advertisers.[62]

With much bigger privacy concerns than Nick Bergus's in mind, fifteen privacy and consumer groups filed a complaint with the Federal Trade Commission against Facebook in May 2010.[63] Along with the fourteen privacy groups that filed the complaint, Senators, news organizations, bloggers, and Facebook members also oppose Facebook's policies.[64] The complaint alleged that Facebook had engaged in unfair and deceptive trade practices and was in violation of consumer protection laws. Specifically, the complaint stated, "[C]hanges to user profile information and the disclosure of user data to third parties without consent 'violate user expectations, diminish user privacy, and contradict Facebook's own representations.'"[65] While some Facebook users may not be very concerned, entities that are highly involved in Internet privacy issues are very worried by Facebook's actions.

---

56. *Id.*

57. *Id.*

58. *Id.* One friend even stated that Nick's post about the lubricant showed up on his Facebook newsfeed every time he logged in. Some of the people who reported seeing the post on their newsfeed were a former co-employee and a coworker's wife. *Id.* For an explanation of what a "sponsored story" is, see *infra* text accompanying notes 101-103.

59. *See id.*

60. Arjun Kulkarni, *How Does Facebook Make Money*, BUZZLE (Jan. 9, 2012), http://www.buzzle.com/articles/how-does-facebook-make-money.html.

61. Frayley v. Facebook, Inc., 820 F. Supp. 2d 785, 792 (N.D. Cal. 2011) (citation omitted).

62. Bergus, *supra* note 54; *see also Frayley*, 830 F. Supp. 2d at 799.

63. *New Facebook Privacy Complaint Filed with Trade Commission*, EPIC.ORG (May 5, 2010), http://epic.org/2010/05/new-facebook-privacy-complaint.html.

64. *Id.*

65. *Id.* (citation omitted).

Although it is still very new, there are growing concerns about the implications of Google's new privacy policy.[66] Jeffrey Chester, an executive director for the privacy advocacy group Center for Digital Democracy, says, "There is no way a user can comprehend the implication of Google collecting across platforms for information about your health, political opinions and financial concerns."[67] Representative Edward J. Markey expressed similar concerns about the way Google will be utilizing users' data across its multitude of services.[68]

It is not just American privacy groups and politicians that have concerns with the manner in which Facebook, Google, and scrapers are using users' data. In March 2012, a German court ruled against Facebook in a suit brought by European privacy groups claiming privacy violations.[69] The court ruled against Facebook for the way it uses its members' e-mail addresses to solicit new users and held that Facebook cannot force its users to grant it a comprehensive license to their content.[70] Facebook is also under fire from German officials for giving itself the right to comprehensive tracking of registered as well as unregistered Facebook members.[71]

Other European courts are also having issues with the implications of Google's new privacy policy. French regulators warned Google that the new privacy policy could violate European Union laws on data protection.[72] The French National Commission, who is investigating potential issues with Google's new privacy policy, stated that the average

---

66. A group of more than thirty attorneys general wrote to Google's Chief Executive Larry Page expressing their concerns with Google's new privacy policy. *See* Julia Angwin, *Web Firms To Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html.

67. *FAQ: Google's New Privacy Policy*, WASH. POST (Jan. 24, 2012), http://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQArw8GOQ_story_1.html.

68. *See id.* Representative Markey is the cochair of the Congressional Privacy Caucus. *Id.*

69. Landgericht Berlin [LG] [Regional Court of Berlin] Mar. 16, 2012, 16 O 551/10, 1 (F.R.G.); *see also* Friedrich Geiger & Shayndi Raice, *Facebook Loses Privacy Case in German Court over Email*, WALL ST. J. (Mar. 6, 2012, 6:44 PM), http://online.wsj.com/article/SB10001424052970203458604577265764008504218.html?mod=WSJ_Tech_LEFTTopNews.

70. *Id.*

71. Elinor Mills, *Facebook Changes "Privacy Policy" to "Data Use,"* CBS NEWS (Mar. 23, 2012, 10:44 AM), http://www.cbsnews.com/8301-501465_162-57403181-501465/facebook-changes-privacy-policy-to-data-use/ (internal quotation marks omitted). Facebook recently added "nonmembers who interact with Facebook" to those who "consent to having personal data transferred to and processed in the U.S." in its Statement of Rights and Responsibilities. *Id.*

72. Jennifer Valentino-DeVries, *Google Privacy Policy Could Violate EU Law, France Says*, WALL ST. J. (Feb. 28, 2012, 5:45 PM), http://blogs.wsj.com/digits/2012/02/28/google-privacy-policy-could-violate-eu-law-france-says/?mod=WSJBlog&mod=blogmod.

user cannot comprehend what Google is doing with their data, which could mean that Google is violating rules requiring companies to inform users about how their information is being utilized.[73] While Google seems responsive to their concerns and has reassured them that its privacy policy changes will comply with European Union laws, it remains to be seen.[74]

IV. HOW COURTS ARE DEALING WITH ONLINE PRIVACY

With the expansion of the Internet and social media, growing privacy concerns have led consumers to look to the courts for help. Unfortunately for many consumers, courts seem unable to provide a remedy for their claims and appear fairly ambivalent towards their plight. In 2001, the United States District Court for the Southern District of New York dismissed plaintiffs' claims relating to invasion of privacy by an online entity.[75] The plaintiffs brought a class action suit against DoubleClick, the Internet's largest advertising corporation.[76] The company's principal service was placing client banner advertisements in front of Internet users who matched the client's target demographic.[77] In order to compile the requisite user profiles to provide this service, Double Click stored cookies on the computer hard drives of any Internet user who accessed Web sites that were either affiliated with DoubleClick or that advertised DoubleClick's clients.[78] The plaintiffs argued that their privacy rights were violated by DoubleClick's use of these cookies to collect consumers' personal information, such as home addresses, telephone numbers, e-mail addresses, names, Web sites visited, and other browsing history used for targeted advertising purposes.[79] The court dismissed all three of the plaintiffs' federal law claims citing, inter alia, that the plaintiffs never suffered a cognizable loss for the collection of their data and that the consumers, by using DoubleClick, consented to the collection of their communications.[80] Furthermore, the court in its reasoning equated Internet advertising with television and newspaper

73. *Id.*
74. *See id.*
75. *In re* DoubleClick Inc., Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).
76. *Id.*
77. *Id.* at 502.
78. *Id.* at 502-03.
79. *See id.* at 503.
80. *Id.* at 500, 514-15, 524-26. The court noted that consumers were able to prevent this information collecting by either requesting an opt-out cookie or reconfiguring their browser so that cookies would be blocked. *See id.* However, in mid-1999, "DoubleClick amended its privacy policy by removing its assurance that information gathered from its users online would not be associated with their personally identifiable information." *Id.* at 505.

advertising, and Internet entities collecting personal data to marketers, retailers, and mail-order catalogs.[81] This often-cited early litigation set the stage for subsequent courts to deny Internet users a right of action under the same reasoning.[82]

Ten years later, in *Bose v. Interclick, Inc.*, the same district court employed much of the same reasoning used in *DoubleClick* to grant the defendant's motion to dismiss most of the plaintiff's claims.[83] In *Bose*, the plaintiff argued that the defendant implanted browser cookies on her computer.[84] These browser cookies differ from flash cookies in that when a user deleted the browser cookie, a flash cookie would respawn the browser cookie "without notice or consent of the user."[85] Furthermore, the plaintiff explained that Interclick employed "history sniffing" codes, which were invisible to the user and would determine and gather the user's prior browsing history.[86]

The plaintiff looked to distinguish her case from *DoubleClick* in that Interclick used and collected her personal information without her permission through these flash cookies and history-sniffing codes.[87] She claimed, "Interclick violated the CFAA by monitoring [the] Plaintiff's web browsing . . . invaded her privacy, misappropriated personal information, and interfered with the operation of her computer."[88] The court was not persuaded.[89] Just as in *DoubleClick*, the *Bose* court found that the plaintiff's allegations did not prove any "cognizable economic losses."[90] The district court further held that the plaintiff failed to show how Interclick deprived her of the economic value of her personal information by collecting and using her personal information.[91]

---

81. *Id.* at 525.

82. *See, e.g.*, La Court v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) (holding that plaintiffs could not show how they were deprived of the economic value of their PII (personally identifiable information) because it was collected by a third party); Bose v. Interclick, Inc., No. 10 CIV. 9183(DAB), 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (holding that invasion of privacy, trespass, and misappropriation of confidential information are not economic losses).

83. *Bose*, 2011 WL 4343517 at *12-14.

84. *See id.* at *1.

85. *Id.*; *see also* text *supra* note 26.

86. *See Bose*, 2011 WL 4343517, at *2.

87. *See id.* at *5.

88. *Id.* at *2 (citation omitted).

89. *See id.* at *3-6.

90. *See id.* (stating that a plaintiff must show at least $5000 of economic loss during any one-year period to prevail on a theory of economic loss and claims such as misappropriation, invasion of privacy, and trespass do not count toward the five thousand dollar threshold for economic losses).

91. *Id.* at *12; *see also* La Court v. Specific Media, Inc., No. SACV 10-1256 GW(JCGX), 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011) (applying similar reasoning as in

In *Claridge v. RockYou*, the United States District Court for the Northern District of California espoused a slightly different view than that put forth by both the *DoubleClick* and *Bose* courts. In that case, the plaintiff sued RockYou, a developer of online applications and services used by social networking sites, for failing to secure and protect its users' personally identifiable information (PII).[92] The plaintiff argued that RockYou failed to apply even the most reasonable and minimal measures to protect its users' personal information and after its security flaw had been exploited and the contents thereof made public in underground hacker forums, the Web site consequently was hacked.[93] The hackers were able to get into RockYou's SQL database and steal all of the user information it contained including the e-mail and social-network login identifications of approximately thirty-two million of RockYou's users.[94]

In dismissing the plaintiff's claim that the defendant violated California's unfair competition law,[95] the district court used reasoning very similar to that asserted in *DoubleClick* and *Bose* in holding that the plaintiff failed to demonstrate any loss of money or property.[96] However, the *Claridge* court diverged from this jurisprudence by proceeding to analyze the plaintiff's three contractual claims.[97] The court denied the defendant's motion to dismiss the plaintiff's claims holding that the plaintiff "sufficiently alleged a general basis for harm by alleging that the breach of his PII has caused him to lose some ascertainable but unidentified 'value' and/or property right inherent in the PII."[98] While unable to determine an exact value, the court refrained from adhering to the rulings of previous courts that espoused the idea that PII had no inherent value and could not be grounds for a cause of action.[99]

Bose that plaintiffs could not show how they were deprived of the economic value of their PII because it was collected by a third party).

92. Claridge v. RockYou Inc., 785 F. Supp. 2d 855, 858-59 (N.D. Cal. 2011).

93. *Id.*

94. *Id.* ("SQL is a database computer language designed for storing data in database management systems.").

95. For example, California's unfair competition law prohibits business practices or acts that are, among other things, injurious to customers, allowing plaintiffs to recover under the law if they can prove they suffered an "injury in fact" and "lost money or property as a result of such unfair competition." Hall v. Time Inc., 70 Cal. Rptr. 3d 466, 467 (Cal. Ct. App. 2008) (citation omitted).

96. *Compare Claridge*, 785 F. Supp. 2d at 867, *with In re* DoubleClick Inc., Privacy Litig., 154 F. Supp. 2d 497, 524-26 (S.D.N.Y. 2001), *and* Bose v. Interclick, Inc., No. 10 Civ. 9183 DAB, 2011 WL 4343517, at *3-6 (S.D.N.Y. Aug. 17, 2011).

97. *Claridge*, 785 F. Supp. 2d at 865.

98. *Id.*

99. *See Bose*, 2011 WL 4343517; *In re DoubleClick Inc.*, 154 F. Supp. 2d 497.

In the same district court as *Claridge*, and less than a year later, Internet users' privacy rights were further protected in a narrowly construed opinion. In *Fraley v. Facebook, Inc.*, the court denied the defendant's motion to dismiss most of the plaintiffs' claims.[100] The plaintiffs sued over defendant's use of a part of the Facebook Web site called "Sponsored Stories."[101] A Sponsored Story is a type of paid advertisement that is generated anytime a member uses the "Like," "Check-in," or "Post" features, plays a game, or uses an application incorporated with the Web site, and Facebook sees the content as relating to an advertiser in some manner.[102] These Sponsored Stories incorporate the member's name, profile picture, a statement that the person "likes" the advertiser, and the company's logo, and then places the endorsement on the member's friends' pages.[103] The plaintiffs contended that Facebook was using their information for its own personal gain without their consent.[104] Facebook countered stating that the plaintiffs implicitly agreed to the use of their information for Sponsored Stories because such use is provided in Facebook's Statements of Rights and Responsibilities. However, the plaintiffs argued that Sponsored Stories were not a Facebook feature when they joined Facebook and further that Facebook never informed them of the changes that would be made to their privacy settings.[105]

This case deviates from previous case law in that the court found that the plaintiffs were actually injured by the Web site's use of their personal information.[106] The court was able to find specific economic injury here mainly because of statements made by Facebook's most important officials.[107] Facebook's CEO, Mark Zuckerberg, stated that "[n]othing influences people more than a recommendation from a trusted

---

100. 830 F. Supp. 2d 785 (N.D. Cal. 2011). The court did however grant the defendant's motion to dismiss the plaintiffs' claim for unjust enrichment citing *Hill v. Roll International Corp.*, where the court of appeals stated, "Unjust enrichment is not a cause of action, just a restitution claim." 128 Cal. Rptr. 3d 109, 118 (2011) (citation omitted).

101. *Frayley*, 830 F. Supp. 2d at 790; *see also supra* note 58.

102. *Frayley*, 830 F. Supp. 2d at 791.

103. *See id.*

104. *See id.* at 792.

105. *See id.*

106. *Compare id. with In re* DoubleClick Inc., Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) (dismissing the claims because the courts were unable to find how the plaintiffs were economically injured), *and In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (same), *and* La Court v. Specific Media, Inc., No. 10-1256-GW, 2011 WL 1661532, at *4 (N.D. Cal. Apr. 28, 2011) (same), *and In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 WL 4403963, at *6 (N.D. Cal. Sept. 20, 2011) (same).

107. *Frayley*, 830 F. Supp. 2d at 799.

friend" and that "[a] trusted referral is the Holy Grail of advertising."[108] Facebook's COO, Sheryl Sandber, further stated, "Marketers have always known that the best recommendation comes from a friend . . . ."[109] The court also relied heavily on assertions by Facebook's CEO and COO that endorsements by friends are two to three times more valuable than generic advertisements sold to the Web site's advertisers.[110] While the opinion should be narrowly construed, it does show that users do have a chance at prevailing in court if they can get over the hurdle of demonstrating that they suffered a specific economic loss through the violation of their privacy rights.

V. COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011

A. Summary

On April 12, 2011, in the wake of mounting concerns of consumers and businesses about how their information and Internet activity were being tracked and used, a bipartisan bill was introduced in the Senate.[111] The Commercial Privacy Bill of Rights Act of 2011, introduced by Senator John Kerry and Senator John McCain, targets the online privacy of consumers.[112] The proposed legislation would establish information protection for consumers similar to the protections set forth in the December 2010 Department of Commerce privacy green paper titled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[113] Both the Department of Commerce's green paper and this newly proposed legislation look to alleviate some of the concerns surrounding information privacy on the Internet, bridging the gap between the lack of online privacy and the lack of legal protections afforded to online privacy.[114]

---

108. *Id.* at 792 (citation omitted).

109. *Id.* at 799 (citation omitted).

110. *Id.* at 800. The court notes that this fact is what distinguishes this case from *Cohen v. Facebook, Inc.* (*Cohen I*), 798 F. Supp. 2d 1090, 1092 (N.D. Cal. 2011) (holding that the plaintiffs were unable to show that their names had any general commercial value), and *Cohen v. Facebook, Inc.* (*Cohen II*), No. C 10-5282-RS, 2011 WL 5117164, at *2 (N.D. Cal. Oct. 27, 2011) (holding that the plaintiffs failed to demonstrate any cognizable injury from Facebook's using their names or likenesses). *Frayley*, 830 F. Supp. 2d at 800.

111. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011), *available at* http://www.opencongress.org/bill/112-s799/show.

112. *Id.*

113. INTERNET POLICY TASK FORCE, U.S. DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

114. *Compare id.* (emphasizing strong protections for privacy of consumers' PII and the relevant role of the FTC in enforcement) *with* S. 799 (same).

Specifically, the bill would provide for consumer notice before Web sites are able to collect personal information that is deemed to be PII.[115] The bill defines PII as the following: first name or initial and last name, address, e-mail address, telephone number (mobile or landline), social security number, credit card number, "[u]nique identifier information that alone can be used to identify a specific individual," and biometric data including fingerprints and retina scans.[116] The bill also states that a consumer's place of birth, date of birth, birth or adoption certificate number, precise geographic location, consumer proprietary network information, or other information that could reasonably be used to identify a consumer when combined with any PII would then become PII and protected.[117]

Aside from requiring that entities give notice to consumers about how PII is used, the bill also calls for entities to provide for opt-out/opt-in consent requirements in order to collect consumer data.[118] Consumers would be given the chance to opt out of having their PII used in a way to which they did not initially agree.[119] Not only would this opt-out requirement apply to the entities themselves, it would also apply to third parties looking to use the individual's information for behavioral marketing or advertising.[120] Additionally, the bill specifically states that these opt-out consent agreements need to be "robust, clear, and conspicuous" for consumers to truly understand and take advantage of their rights.[121]

The opt-in consent requirements would be necessary under two circumstances.[122] The first is for the collection, use, or transfer of "sensitive personally identifiable information."[123] Sensitive PII is information that, if disclosed without the consumer's authorization, carries a significant risk of economic or physical harm; such information includes medical information and religious affiliation.[124] The second circumstance necessitating the opt-in requirement occurs when an entity intends to use or transfer a consumer's previously collected PII after a substantial change to the entity's privacy policy.[125]

---

115. *See* S. 799 § 201.
116. *Id.* § 3.
117. *Id.*
118. *Id.* § 202.
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.*
124. *Id.* § 3.
125. *See id.* § 202.

Not only does the bill spell out what it is seeking to protect, it explains how it intends to do so. The Federal Trade Commission (FTC) would be tasked with the bill's enforcement.[126] The FTC would be able to enforce the bill's requirements against any business that "collects, uses, transfers, or stores" PII of more than 5,000 consumers a year.[127] To comply with the requirements set out by the bill, the FTC will need to promulgate rules requiring entities to implement security measures that protect consumers' PII.[128] The bill states that violators could be looking at as much as $16,500 in civil penalties for each violation, with the maximum civil penalty being $3 million.[129]

While the bill sets out penalties that entities will face for violating the Act's requirements, it provides no recourse for individuals to bring suit.[130] The bill also takes away many enforcement mechanisms from the states. State Attorneys General would be able to conduct investigations and bring civil actions against entities that are in violation of the bill, but they would not be able to enforce the bill's provisions concurrently with the FTC.[131] The States' Attorneys General would also be forced to give the FTC notice before beginning any civil action under the bill.[132] Similarly, the bill would preempt any state laws, except for those that deal with "the collection, use, or disclosure of health or financial information[,] . . . notification requirements in the event of a data breach[,] . . . or acts of fraud."[133]

Though the FTC would deal with much of the bill in the beginning, a year after its enactment the FTC would be required to facilitate the creation of a self-regulatory safe harbor program.[134] The safe harbor program would be subject to FTC oversight, but a substantial role in the development and implementation of the program would be delegated to the United States Department of Commerce.[135] The Department of Commerce would also have an ongoing role in creating data sharing policies domestically and with other nations.[136]

---

126. *Id.* § 402.
127. *See id.* § 401.
128. *Id.* § 402.
129. *Id.* § 404.
130. *Id.* § 406.
131. *Id.* § 403.
132. *Id.*
133. *Id.* § 405.
134. *Id.* § 501.
135. *See id.* § 701.
136. *Id.*

B. Criticisms of the Bill

While this new bill certainly seems to be a step in the right direction to protect the privacy rights of consumers, notable critics say it falls short.[137] Some of the more vocal critics of the bill have been Consumer Watchdog, the Center for Digital Democracy, Consumer Action, Privacy Rights Clearinghouse, and *Privacy Times*. These groups banded together to write a letter to Senator John Kerry and Senator John McCain explaining why they could not and would not support this bill.[138] The first grievance the opponents had was with the lack of a "do not track" mechanism.[139] Such a mechanism would give consumers the right to choose if they want their private information to be gathered or used by any companies that track consumer online activity.[140] The concept of a "do not track" mechanism is analogous to a "do not call" list which prevents telemarketers from calling people who are on the list.[141] Not only are the critics of Senators Kerry and McCain's bill calling for a "do not track" option, the American people are as well.[142] In a poll by Consumer Watchdog in July 2010, it was found that eighty-six percent of Americans support a "do not track" option.[143]

Critics also cite the "notice and choice" model the bill employs as another reason for their inability to support the bill.[144] The notice and choice model allows entities to have privacy policies of which consumers can opt out.[145] The problem with this model is that it allows entities to create lengthy privacy policies full of legal jargon incomprehensible to most of its consumers.[146] This form of self-regulation has proved

---

137. *See* John M. Simpson, Jeff Chester & Carmen Balber, *Consumer Groups Welcome Bipartisan Effort, but Warn Kerry-McCain Bill Insufficient To Protect Consumers' Online Privacy*, CONSUMER WATCHDOG (Apr. 12, 2011), http://www.consumerwatchdog.org/newsrelease/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-pr.

138. *See id.*

139. *See id.* A new "Do Not Track Me" bill was introduced to Congress on February 11, 2011, by Representative Jackie Speier. Carmen Balber & John M. Simpson, *Landmark "Do Not Track Me" Bill To Block Unwanted Spying on the Internet, Says Consumer Watchdog*, CONSUMER WATCHDOG (Feb. 11, 2011), http://www.consumerwatchdog.org/newsrelease/landmark-do-not-track-me-bill-block-unwanted-spying-internet-says-consumer-watchdog/. The new bill is the first bill to explicitly call for a "do not track me" mechanism.

140. Balber & Simpson, *supra* note 139.

141. *Id.*

142. *See* Carmen Balber & John M. Simpson, *Consumer Watchdog Poll Finds Concern About Google's Wi-Spy Snooping*, CONSUMER WATCHDOG (July 27, 2010), http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-poll-finds-concern-about-googles-wi-spy-snooping/.

143. *Id.*

144. *See* Simpson, Chester & Balber, *supra* note 137.

145. *See id.*

146. *See id.*

ineffective, and critics are calling for a change.[147] Likewise, it is argued that the bill is actually stripping consumers of some of the safeguards they previously enjoyed.[148] Private rights of action are specifically done away with in the new bill.[149] Allowing a private right of action is important, because it ensures that privacy protections are actually being enforced.[150] States would also be preempted from affording its citizens a higher level of protection than that allowed under the bill.[151]

Also very disconcerting to many is the "established business relationship" exception that the bill creates.[152] The bill defines an "established business relationship" as anytime a consumer creates an account with an entity and uses the account for the receipt of products or services that the entity offers.[153] Essentially, some of the entities that consumers are most worried about with regard to information privacy, such as Google, Twitter, and Facebook, would be exempt under this exception.[154] This would allow Facebook, for example, to take any of its users' PII and use it for targeted advertising, because Facebook would not be seen as a "third party."[155]

VI. CONCLUSION

A. What Needs To Occur To Ensure Privacy

It is clear that politicians, bloggers, and users all think that Web sites have crossed the line with regard to their privacy policies and how the Web sites are using their users' personal information. Politicians are taking the necessary steps to prohibit such actions by proposing the Commercial Privacy Bill of Rights Act of 2011, but they are not going far enough.

Just as other critics have stated, Web sites should be forced to utilize opt-in methods for privacy rather than opt-out. Many people have a hard time navigating Web sites such as Facebook, let alone finding out how

147. *See id.*
148. *See id.*
149. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 406 (2011).
150. *Id.*
151. *See id.* Critics also have issues with the bill's taking away much of the FTC's regulatory power and giving it to the Commerce Department. *See id.* Critics explain that the Commerce Department is principally concerned with the promotion of business interests and thus should not be the federal body entrusted to protect the interests of consumers. *Id.*
152. *See* Venkat, *A Look at the Commercial Privacy Bill of Rights Act of 2011*, TECH. & MARKETING L. BLOG (Apr. 20, 2011, 9:03 AM), http://blog.ericgoldman.org/archives/2011/04/.
153. *See id.*
154. *Id.*
155. *See id.*

their data could possibly be used and figuring out how to disable such usage. No person should have to go to such great lengths to keep their personal and sometimes very private information from being sent or sold to third parties. If there were opt-in mechanisms, the Web sites would not be completely precluded from using members' data; they would just need to get more explicit consent for such use. Likewise, if users do not mind having their data used, they can simply press a button opting in to that specific type of use. Having an opt-in rather than an opt-out mechanism would allow users to understand to what they are agreeing.

Similar to the privacy granted by an opt-in mechanism is a "do not track" button, which was left out of the new Commercial Privacy Bill of Rights Act of 2011 even though it had previously been suggested by the Federal Trade Commission, privacy groups, and other politicians.[156] Some of the most influential Internet companies, such as Google and Mozilla, agree with the need for a "do not track" button.[157] When implemented by these companies, the "do not track" button will put a stop to these Internet companies utilizing users' data about their "Web browsing habits to customize ads . . . for employment, credit, health-care or insurance purposes."[158] However, users' data will still be used for certain purposes such as product development, market research, and to help law enforcement officials.[159] If these large Internet companies stay on track and honor the "do not track" button as they promise, it will be a very large step in the right direction. It will be a step towards putting users' privacy back in their own hands.

Along with it being necessary for users to opt in to privacy options or be able to select a "do not track" button, it is also necessary for users to understand the various privacy policies and when and how these policies change. Currently, many companies have privacy policies for their Web sites that are so long and riddled with legal jargon that the average person has neither the time nor ability to truly comprehend their terms.[160] Take Facebook for example: even if a user is able to ascertain from the privacy policy that he needs to utilize opt-out mechanisms in order to keep his information private, he would need to click through

---

156. *See* Angwin, *supra* note 66.

157. *See id.*

158. *Id.*

159. *See id.*

160. Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES (May 12, 2010), http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html. For example, Facebook's privacy policy is longer than the United States Constitution. *Id.* The "Help Center" available to users is not of much help either, forcing a user to sift through more than 45,000 words to try to find an answer to a question. *Id.*

more than fifty privacy buttons which entails choosing from among more than 170 options.[161] Making users go to such extremes to keep their information private should not be allowed. Considering the statement made by Facebook's CEO detailing the profitability of the company's use of member-data, it seems far from accidental that opting out of privacy settings is unnecessarily complicated.

In addition to establishing privacy settings that are shorter and easier to understand, companies should be required to inform users anytime there is a change to its privacy policies. From a user's point of view, it is utterly deceptive for companies such as Facebook to change its privacy policies without notifying users, especially when those changes make public settings that a user explicitly set as private. Now, social media Web sites are more than just a way to contact old friends; members are "friends" with their parents, coworkers, employers, priests, and any number of other acquaintances. Therefore, such a change could be very damaging to not only their social life, but their work life as well. With such potential ramifications, deceptive practices of companies modifying their policies without alerting their users to those changes should be illegal.

In addition to enacting new measures that ensure users understand privacy policies that put users in charge of their personal information, the legislature should consider implementing a new privacy tort for violations of their online privacy. As the laws currently stand, users often are not able to succeed in court, because they are unable to show concretely how they were economically hurt by a Web site using and distributing their data.[162] Users should have some sort of redress in court without having to prove economic damages.

However, a higher probability of user's chances to prevail in court is only half the battle. It is also imperative that users have the requisite standing to bring Internet companies to court. In the new Commercial Privacy Bill of Rights Act of 2011, politicians look to explicitly exclude a private cause of action for companies breaching its users' privacy rights.[163] Under the Act, there would be no private cause of action, because companies would be federally regulated; but Web sites that have fewer than 5,000 members are not included and would essentially be

---

161. *Id.*

162. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 499-500 (S.D.N.Y. 2001); Claridge v. RockYou Inc., 785 F. Supp. 2d 855 (N.D. Cal. 2011); Bose v. Interclick, Inc., No. 10 Civ. 9183 DAB, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011).

163. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 406 (2011).

untouchable.[164] It does not make sense that simply because a Web site is small or just starting, it cannot be liable to anyone if it violates the privacy of its members.

B. Ways Users Can Protect Themselves in the Meantime

There are some general ways in which users can protect themselves and increase their online privacy. First, it is important for users to monitor the cookies being placed on their computers. While some cookies are helpful and at times even necessary for a Web site to work properly, many are simply used to gather the user's data and should be deleted.[165] Second, a user should create a "side" e-mail account.[166] Side e-mail accounts are very important when using public forums on the Internet, e-mailing a company or person a user does not know, or signing up for things online.[167] Using side accounts decreases the number of spammers and tracking services invading your real account, which would contain all of a user's more private information and communications.[168] A final way in which users should increase their online privacy is to use different pseudonyms in e-mail addresses and user names that are not too closely connected to each other or closely related to the users' personal information.[169] Differing and difficult-to-decipher pseudonyms make it more challenging for scrapers to find out who a user really is.[170]

For example, with so much criticism of and concern for Google's new privacy policy, many are asking if there is anything they can do to insure that their information is not being collected and used. One measure a user can take is to stop using Google altogether, but that would mean a user would have to stop using Google Search, Gmail, and all of the rest of Google related services. The other measure users can take is to "pause" their Web history. This does not remove cookies that Google places on users' computers; it simply pauses Google's compilation of their information.[171] Furthermore, even if users do this, there is no guarantee that Google will not turn it back on when it sees fit or that

---

164. *Id.* §§ 401, 406.

165. *See* Stanton McCandlish, *EFF's Top 12 Ways To Protect Your Online Privacy*, ELECTRONIC FRONTIER FOUND. (Apr. 10, 2002), https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy. A side e-mail account is an alternative e-mail address, separate from a main e-mail address.

166. *Id.*

167. *See id.*

168. *See id.*

169. *Id.*

170. *See id.*

171. Andrew Couts, *How To: Delete Your Google Web History*, DIGITAL TRENDS (Feb. 23, 2012), http://www.digitaltrends.com/web/how-to-delete-your-google-web-history/.

Google is not retaining a user's information that was already collected. All it means is that for a period of time, a user's history is not collected and used.[172] For users to "pause" Google's compilation of their information, users first must go to google.com/history, log in, and then make sure to press the "pause" button and not the "turn Web history off" button.[173]

While it is possible to suggest remedies for current issues with online privacy, the most important way for users to ensure their privacy is to stay educated. With technology and the Internet constantly changing, staying up-to-date with those changes is really the only way users can ensure that their information is being kept private.

172. *Id.*
173. *Id.*