UIC John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 4 *Journal of Computer & Information Law - Symposium 2012*

Article 4

Fall 2012

What's Mine is Yours: Targeting Privacy Issues and Determining the Best Solutions for Behavioral Advertising, 29 J. Marshall J. Computer & Info. L. 637 (2012)

Sarah Cathryn Brandon

COMMENT

WHAT'S MINE IS YOURS: TARGETING PRIVACY ISSUES AND DETERMINING THE BEST SOLUTIONS FOR BEHAVIORAL ADVERTISING

SARAH CATHRYN BRANDON[1]

I. INTRODUCTION

A recent Gallup poll suggests that two-thirds of Americans who use the Internet would prefer to not have their browsing history stored and then used for purposes of targeted, or behavioral, advertising.[2] In fact, most responded that they would be unwilling to give up the privacy that is potentially compromised via data-storage in exchange for free content.[3] However, people engage in products that are free on the Internet all the time, Facebook and Google are probably the best examples.[4] Arguably, Facebook would cease to exist if it did not store one's personal information in order to save one's profile.[5] However, the real issue for people is not the purported purposes for which their information is being obtained; rather it is that some advertising companies track browser history and retain consumers' private information from those site visits without consent.[6]

---

1. J.D. Candidate, May 2013; B.A., The University of Texas at Austin. I would like to thank my friends on the JCIL Staff for all their help and support. I would also like to thank my brand new husband, Brian, for being so supportive of everything I've ever done and for listening to me read this comment out loud so many times.

2. Daniel Indiviglio, *Most Internet Users Willing to Pay for Privacy*, ATLANTIC (Dec. 22, 2010, 4:04 PM), http://www.theatlantic.com/business/archive/2010/12/most-internet-users-willing-to-pay-for-privacy/68443/.

3. *Id.*

4. Julie Brill, *Competition and Consumer Protection: Strange Bedfellows or Best Friends?*, 10 ANTITRUST SOURCE 1, 7 (2010).

5. *Id.*

6. Indiviglio, *supra* note 2.

A woman that announces her wedding engagement on Facebook can certainly expect advertisements for engagement rings, photographers, and dresses.[7] Though she chose to announce her personal information, it might not necessarily follow that Facebook should retain that information indefinitely for purposes aside from social networking.[8] However, there is usually not a traceable economic loss or physical injury that results from obtaining and storing personal data.[9] This is evidenced by the fact that courts have mostly rejected plaintiffs' claims concerning privacy issues resulting from the use of "cookies," a tool used to store data on computers.[10]

There are already laws against intercepting information via e-mail, regular post mail, and telephone wiretapping without consent.[11] However, new concerns arise in the context of behavioral advertising since data storage can exists for decades and potentially store an infinite amount of data.[12] But is it merely a strange feeling associated with the thought that one's personal and private information is stored for potentially decades?[13] Or is there an actual harm that stems from advertising practices that retain seemingly innocuous information, such as browser history or personal information that is essentially public record?[14]

At this point, it seems that privacy protection for purposes of behavioral advertising is at a standstill.[15] What is the purpose of regulating how long a company can store data if there is no harm to be recognized by a court of law?[16] One argument is that there is little privacy risk involved and consumers receive a benefit from targeted advertising; therefore, courts are unwilling to afford much relief to plaintiffs, as it would

---

7. Catherine Schmierer, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 17 RICH. J.L. & TECH. 13, 1 (2011).

8. *Id.*

9. Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *10 (S.D.N.Y. Sept. 17, 2011). This assumes that the information is only used for behavioral advertising and not so third parties could intercept the information, which will be shown later can happen. *See also* Hirsch, *supra* note 9, at 446.

10. *Bose*, 2011 WL 4343517, at *28.

11. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 225 (1996).

12. James Schedwin, *Behavioral Targeting: Issues Involving the Microsoft-Aquantive and Google-DoubleClick Mergers, and the Current and Proposed Solutions to those Issues*, 4 J. L. & POL'Y FOR INFO. SOC'Y 704, 711 (2009).

13. Schmierer, *supra* note 7, at 1 (the issue is that this seems to go beyond the purposes of targeted advertising); s*ee also* Eric Goldman, *Flash Cookies Lawsuit Tossed for Lack of Harm—La Court v. Specific Media*, TECH. & MARKETING L. BLOG (May 4, 2011), http://blog.ericgoldman.org/archives/2011/05/Flash_cookies_l.htm.

14. Eric C. Bosset, et al., *Private Actions Challenging Online Data Collection Practices Are Increasing: Assessing the Legal Landscape*, 23 INTELL. PROP. & TECH. L. J. 3, 4 (2011).

15. *Id.*

16. La Court v. Specific Media, Inc., 2011 WL 2473399, at *9 (C.D. Cal. Apr. 18, 2011).

seem out of balance with the benefit conferred along with such slight possible risk.[17] However, plaintiffs still feel wronged and have not been deterred from bringing suit.[18] The reality is that there is more at risk than is perceived.[19] There are at least two potential harms that this comment argues should be recognized besides economic harms. The first is the loss of personal dignity, and the second exists when unwanted third parties intercept personal information.[20]

The Background section will begin with an overview of the issues associated with behavioral advertising so far, which will segue into a brief discussion of how cookies actually function in order to track browser history. Following will be a summary of the case law and the common law legal theories that plaintiffs have used in court that will be further analyzed in the Analysis section. There will then be a brief introductory discussing the history of the Federal Trade Commission (FTC), its authority, and how it has approached behavioral advertising. This will be followed by Congress' approach to privacy concerns in the behavioral advertising arena, including a specific discussion about the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, as well as the newly proposed "Do Not Track" Bill.

The Analysis section will include the argument that there are two harms that should be acknowledged and protected. This comment seeks to then rank each of the legal theories that plaintiffs have brought, and which one will protect those potential harms the most. The most preferred way to protect consumers would be for the FTC to adopt its proposed "privacy by design" framework. This comment will also conclude, however, that trespass to chattels claims should have some viability. A slightly less preferred alternative is proposed, as well, which would amend the current Computer Fraud and Abuse Act and the Electronics Communication Act to include a cause of action for plaintiffs with no economic loss. The last alternative, not embraced at all, is for Congress to enact new legislation that attempts to protect consumers.

II. BACKGROUND

A. The Harms Associated with Behavioral Advertising

A problem that plaintiffs are running into is whether the issues they

17. Brief for Respondents at 9, Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011) No. 10-779.

18. Schedwin, *supra* note 12, at 711.

19. Brian Stallworth, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, 62 Fed. Comm. L.J. 465, 473 (2010).

20. Slade Bond, *Doctor Zuckerberg: Or, How I Learned to Stop Worrying and Love Behavioral Advertising,* 20 Kan. J.L. & Pub. Pol'y. 129, 136 (2010).

bring before any court are viable or not.[21] Some suggest that the privacy risks involved in targeted advertising are minimal since no actual person gets ahold of the information because it is tracked, stored, and used for advertisements via cookies.[22] Others have argued that this does not close the door to third parties to intercept information, whether it is criminals or even the government.[23] The latter group argues that people's most private inquiries are stored for an indefinite amount of time in search engines, allowing people to link the searches back to a particular user.[24] The comprehensive user profiles that are created make it more likely that a person is able to be identified, thus allowing the third party that intercepted the information on the profile to commit fraud, identity theft, or a host of other criminal activities.[25] However, it is difficult for protections to be in place when courts and scholars refuse to acknowledge the privacy implications of behavioral advertising.[26]

Moreover, courts have mostly required an economic or tangible loss.[27] This means that most of the cases have been dismissed simply because the plaintiffs could not establish that they incurred a monetary loss due to their personal information being tracked.[28] This means that privacy concerns are being defined monetarily, while personal choice and the potential for information to fall into the wrong hands are being discounted as legitimate harms.[29] The FTC's previous methods for addressing the privacy concerns consumers had over behavioral advertising self-admittedly did little to protect them because it focused on economic harms, as well.[30] This indicates the FTC's willingness to embrace a model that identifies more than monetary harms.[31]

There are at least two harms that should be recognized by courts that this comment espouses.[32] The first is personal autonomy and dignity, which reflects consumer choice and privacy.[33] This is especially important with flash cookies because oftentimes the consumer has deleted

21. Stallworth, *supra* note 19, at 473.
22. Goldman, *supra* note 13.
23. *See* Hirsch, *supra* note 9, at 444.
24. *Id.* at 445.
25. *Id.* at 446.
26. Bosset, et al., *supra* note 14, at 4.
27. *La Court*, 2011 WL 2473399, at *7.
28. *Id.*
29. Interview by John Villfranco with David Vladeck, Director, FTC Bureau of Consumer Protection (Mar. 19, 2010); *see* http://www.kelleydrye.com/publications/articles/1361/_res/id=Files/index=0/Villafranco_Interview%20with%20David%20Vladeck_Apiril%202010.pdf.
30. *Id.*
31. *Id.*
32. Bond, *supra* note 20, at 136.
33. *Id.*

browser cookies, indicating his desire to not be tracked.[34] Flash cookies eliminate consumer choice to not be tracked, as well as personal dignity by tracking personal information anyway.[35] The second harm, which has already been mentioned, is the potential for unwanted third parties to intercept information.[36] This can happen by third party advertisers that have used flash cookies to obtain personal information, hackers, or the government without obtaining a warrant.[37]

B. How Cookies Work

Targeted advertising is the process by which a company, via a cookie, tracks a person's browser history and collects personal information in order to direct specific advertisements better suited to that person's tastes.[38] The companies that engage in this are usually network advertisers that enter into contracts with website owners, where the websites track user data and allow the advertising network to then use the data to direct specific advertisements back to the user on its own website.[39] This type of advertising cuts out the guess work for businesses and allows them to deliver ads containing specific products similar to what someone has searched for before or what they might be interested in in the future based on the types of searches performed.[40]

A cookie is a file that is placed on the hardware of a consumer's computer.[41] They are used to store passwords and usernames for a site one may visit.[42] However, they are also able to track one's web history across multiple sites, store information from each of these, and combine it so that companies can then direct ads suited to that person based on his web activities.[43] Cookies can store information for decades and end up in massive databases that store private data.[44] These databases are profiles that are constructed in order to store the information on a particular consumer, and are used to redirect ads at the consumer based on the information stored in the data base.[45]

There are two types of cookies used that allow a company to engage in behavioral advertising.[46] A "browser cookie" simply tracks browser

34. Schmierer, *supra* note 7, at 15.
35. Bond, *supra* note 20, at 136.
36. *See* Hirsch, *supra* note 9, at 444.
37. *Id.*
38. Schmierer, *supra* note 7, at 14.
39. *See* Hirsch, *supra* note 9, at 447.
40. Schmierer, *supra* note 7, at 12.
41. Schedwin, *supra* note 12, at 711.
42. Schmierer, *supra* note 7, at 14.
43. *Bose*, 2011 WL 4343517, at *3.
44. Schedwin, *supra* note 12, at 711.
45. Bond, *supra* note 20, at 133.
46. Schmierer, *supra* note 7, at 15.

history, and can be disabled and deleted by the consumer in the browser settings on her computer so that her web history will no longer be tracked.[47] A "flash cookie," on the other hand, is used to "respawn" a browser cookie.[48] The user has no notice that the flash cookie is being engaged or that the browser cookie is reinstalled.[49] Rather, once the user has actively chosen to not have her information tracked by disabling the browser cookies, her choice is effectively moot once a flash cookie re-enables the browser cookie.[50]

C. FTC, Congress, and Courts' Approaches

1. *History of the FTC and its Approaches to Privacy*

Consumer choice and protection was not at the forefront of the Federal Trade Commission's mission when it was created in 1914 by the Federal Trade Commission Act.[51] Rather, it was primarily to ensure businesses engaged in fair competition.[52] The Federal Trade Commission Act was later amended in 1938 by adding Section 5, which gave broad authority to the FTC.[53] This amendment allowed the FTC to regulate all "unfair and deceptive acts or practices," which then covered consumer protection, as well as businesses.[54] The amendment also allowed the FTC greater flexibility when approaching problems, which means that it is theoretically able to look at consumers' issues on a case-by-case basis and address their specific concerns.[55]

The FTC does not have jurisdiction over all companies, though the ones that are within its authority are subject to the frameworks and policies that it puts into place.[56] The statutes granting enforcement authority to the FTC are: Federal Trade Commission Act, Children's Online

47. Indiana University Information Technology Services, http://kb.iu.edu/data/ahic.html (last visited Nov. 26, 2011).

48. Schmierer, *supra* note 7, at 15.

49. *Id.*

50. *La Court*, 2011 WL 2473399, at *2.

51. Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 San Diego L. Rev. 809, 814 (2011) (noting the Act was passed concurrently with the nation's first antitrust law, the Clayton Act, reinforcing the FTC's original purpose focusing on businesses).

52. *About the Federal Trade Commission*, Federal Trade Commission, (Nov. 13, 2011) http://www.ftc.gov/ftc/about.shtm.

53. *Id.*

54. Andrew B. Serwin, et al., Privacy, Security, and Information Management: An Overview 422 (2011).

55. *Id.* at 421.

56. *About the Federal Trade Commission*, *supra* note 52 ("Exempt from the FTC's jurisdiction are many types of financial institutions, airlines, telecommunications carriers and other types of entities."); *see* Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 102 (2011).

Privacy Protection Act, Gramm-Leach-Billey Act, Telemarketing and Consumer Fraud Abuse Prevention Act, and the Fair Crediting Reporting Act.[57] The recent "Do Not Track" Act proposed by Senator Rockefeller to give consumers better means of opting out of being tracked includes a provision stating that enforcement will be accomplished via the FTC.[58]

In 2000, the FTC adopted a "notice-and-choice" model to approach consumer privacy, which charged companies with developing privacy notices that would better inform the consumer of their practices so the consumers could make an informed decision.[59] This became problematic because although the consumer had the ability to read the policies, the agreements still did not provide much consumer control.[60] Furthermore, the policies still became more complex over time, burdening consumers with having to read lengthy policies they had little control over to begin with.[61]

Wanting to adopt a policy that better reflected consumer concerns, the FTC then promoted the "harm-based model," which focused more specifically on the harms that the consumer actually encountered.[62] However, this approach did little to remedy the issues with the previous approach and came with its own problems.[63] Within this framework, the FTC focused less on what was actually agreed to in the privacy policy and instead on the actual injury the consumer suffered later on due to either a breach or because of an unfair policy.[64] This had two effects: (i) it still did not allow consumer control or mandate clearer privacy policies; and (ii) it required the consumer to show a "substantial" harm, often an economic one.[65]

Finally, and more recently, the FTC has looked at a "privacy by design" framework, which recognized more readily that there are other

57. SOLOVE & SCHWARTZ, *supra* note 56, at 102.

58. S. 913, 112th Cong. §2 (2011). Most bills proposed by Congress would enforce stricter regulations through the FTC. *See* Hirsch, *supra* note 9, at 452.

59. Serwin, *supra* note 51, at 815.

60. Schmierer, *supra* note 7, at 41.

61. Serwin, *supra* note 51, at 815

62. *Id.*

63. *Id.*

64. Stallworth, *supra* note 19, at 491.

65. Serwin, *supra* note 51, at 815 (quoting "substantial" from FTC v. Accusearch Inc., 570 F.3d 1193, 1190-1206 (10th Cir. 2009) (describing when a website sold various personal data, including telephone records, the FTC brought suit against the website, Accusearch, Inc., and its president and owner to stop the sale of confidential information and to require it to disgorge its profits from any sales that had already taken place). "Substantial" in this case constituted the emotional harm associated with stalking or harassment and the costs associated with changing telephone providers. *Id.*

harms besides economic ones.[66] However, these types of harms, such as personal dignity and the possibility of third parties intercepting private information have not yet been acknowledged by most courts.[67] Courts still seem hesitant to recognize that someone can be harmed simply because his browser history is tracked and information from that history is stored.[68] The privacy by design framework would take a more regulatory approach by asking companies to fulfill certain measures such as retaining data for a certain purpose and only for as long as necessary to fulfill that purpose.[69] It also seems the most apt to accomplish what Professor Daniel Solove from George Washington University Law School has advocated, which is a method that "prevent[s] harms from arising rather than merely providing remedies when harms occur."[70]

With behavioral advertising, the FTC has noted the benefit that consumers themselves receive from targeted advertisements, apart from the one that companies get by directing ads to a specific group of people that are more likely to be receptive to those products.[71] The FTC therefore designed an approach to consumer privacy that would allow consumers and companies to still engage in this symbiotic relationship while providing a framework for consumers to feel protected.[72] This approach favors "self-regulation" that focuses on ensuring consumers receive adequate notice that they are being tracked and allows for them to consent by continuing to browse the web or disabling the cookies themselves.[73] This will allow companies to utilize policies that provide protection without "stifling innovation where privacy concerns are minimal."[74]

The FTC's approach has shifted slightly as technology has developed, citing newer developments in privacy issues.[75] In a 2010 interview with FTC Director David Vladeck, he noted that the harm-based frameworks "do not promise to serve us well in the future."[76] He added that the FTC should focus more on principles that "guide us as we move

66. James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls of Just More Notice and Choice?*, 37 WM. MITCHELL L. REV. 1727, 1732 (2011).

67. *Bose*, 2011 WL 4343517, at *28.

68. *Id.*

69. Nehf, *supra* note 66, at 1732.

70. Serwin, *supra* note 51, at n. 14 (citing Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1242 (2003)).

71. Schmierer, *supra* note 7, at 33.

72. Brill, *supra* note 4, at 7-9.

73. Schmierer, *supra* note 7, at 58.

74. Interview by John Villfranco, *supra* note 29.

75. *Id.*

76. *Id.*

forward," attributing this to how quickly technology develops.[77] It should be noted that the FTC has also repeatedly called for Congress to consider some type of "do not track" legislation.[78]

2. *Legislation v. Market Regulation*

Proponents of government regulation argue that legislation can set specific rules and guidelines that, with the force of law, would force companies to put privacy ahead of profits.[79] This usually means that Congress enacts legislation that is enforced by the FTC.[80] Some bills would require privacy policies to be clear, "provide users with meaningful choices," and require actual consent before the website could start tracking one's information.[81] Online marketing firm, Ad Age Digital, laid out three reasons for why it advocated do-not-track legislation (though not specifically the "Do Not Track" Act of 2011).[82] They were as follows:

> First and foremost, it is the right thing for consumers. Many consumers just do not like being tracked. We should respect this, and let them opt out. Second, done right, legislation will incentivize innovation, as well as the adoption of best practices. Third and far from least, a good law, by making consumers feel safe, will help big brands feel comfortable spending online.[83]

Opponents argue that Congress does not understand privacy better than the market, and that legislation, besides being slow to enact, has difficulties keeping up with technological changes.[84] Privacy law and targeted advertising are unique because newer privacy concerns arise out of newer devices and technologies.[85] What were once privacy con-

77. *Id.* (these comments also reflect the FTC's stance on "formal regulations on privacy," which are not embraced because of rapid technological innovation).

78. *FTC Testifies on Efforts to Protect Consumer Privacy*, FEDERAL TRADE COMMISSION (May 9, 2012), http://www.ftc.gov/opa/2012/05/donottrack.shtm. The FTC has also considered implementing a "do not track" mechanism, similar to the "do not call" registry that would allow consumers to opt out of being tracked, without requiring the government to maintain a list of participants. This proposal, to date, has not been decided on yet. Oddly, it would most likely require the use of a persistent cookie to function. This comment does not discuss the "do not track" mechanism, but does note that it is probably at odds with the privacy by design approach embraced here. *See FTC Resources for Reporters, The Do Not Track Option: Giving Consumers a Choice*, FEDERAL TRADE COMMISSION (Aug. 28, 2012) http://www.ftc.gov/opa/reporter/privacy/donottrack.shtml.

79. *See* Hirsch, *supra* note 9, at 452.

80. *Id.*

81. *See* Hirsch, *supra* note 9, at 453.

82. Steven Vine, *Meet the Big Online Marketing Firm That Wants 'Do-Not-Track' Legislation*, AD AGE DIGITAL (Aug. 12, 2010), http://adage.com/article/digitalnext/meet-big-online-marketing-firm-track-legislation/145346/.

83. *Id.*

84. *See* Hirsch, *supra* note 9, at 453.

85. Stallworth, *supra* note 19, at 469.

cerns over desktops and laptops is now extended to hand-held devices.[86] Moreover, market regulation proponents argue that companies are better able to address more quickly privacy concerns because they understand their product best and can incorporate solutions into the competition.[87] Furthermore, they are better able to more efficiently accommodate when technologies become obsolete or evolve into newer products with different technology.[88] FTC Director David Vladeck has noted that: "[The FTC is] spending a lot of [its] time now thinking about mobile applications because the reality is, within five years, mobile smart phones, iPads, and PDAs are going to dominate the marketplace, and laptops may be an anachronism."[89]

The middle ground to this is self-regulation, which the FTC has mostly embraced.[90] This, exponents argue, allows for a more rapid adjustment to newer technologies since companies know their policies and businesses better than anyone else.[91] This is accomplished while simultaneously establishing a privacy framework that ensures consumers are adequately protected.[92]

Recently, Congress has felt the need to do more in the behavioral advertising arena, and several members of Congress have put forth their versions of bills that would afford protection.[93] Most of the bills have focused on regulating the actual collection and use of data.[94] A recent bill, dubbed the "Do Not Track" Bill, was proposed by Senator Rockefeller out of concern that "companies have too much freedom to collect user data on the Internet," and is unique because it includes a provision that extends protection to mobile devices.[95] This type of regulatory approach seems to codify what the FTC has tried to propose in the past, focusing on clear and concise notices, but adds an "opt-out" feature that enables the consumer to still visit a website without being tracked.[96] The FTC has asked Congress before to enact legislation that would accomplish

86. S. 913.

87. Brill, *supra* note 4, at 48.

88. Interview by John Villfranco, *supra* note 29.

89. *Id.*

90. Schedwin, *supra* note 12, at 711.

91. Nehf, *supra* note 66, at 1729.

92. *Id.*

93. Schmierer, *supra* note 7, at 50. The bills mentioned in this article are the Boucher-Stearns Privacy Discussion Draft and the Best Practices Act, introduced by Representative Bobby Rush. *Id*. The prior had more accountability mechanisms built in which, the article notes, "dovetail[ed] the industry's efforts to increase the accountability in online behavioral advertising through new compliance programs." *Id.*

94. *See* Hirsch, *supra* note 9, at 453.

95. Cecelia Kang, *Sen. Rockefeller Introduces "Do Not Track" Bill for Internet*, POST TECH (May 9, 2011, 4:23 PM), http://www.washingtonpost.com/blogs/post-tech/post/sen-rockefeller-introduces-do-not-track-bill-for-internet/2011/05/09/AF0ymjaG_blog.html.

96. S. 913.

these goals, but in the meantime requires companies to adhere to whatever self-regulations they have imposed on themselves within the context of the goals the FTC has set forth.[97]

Congress has enacted laws before that have afforded privacy protection to consumers.[98] The two that this comment focuses on are the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA). Both were enacted long before the electronic version of targeted advertising was even thought to exist.[99] Though both have been effective in providing relief in certain circumstances, they have so far proven inapplicable to claims where plaintiffs complain that their personal information was tracked and stored.[100]

The CFAA, enacted in 1986, was specifically intended to combat criminal computer hacking by prohibiting and punishing unauthorized access to computers.[101] It also has a civil remedy, which states that "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages or injunctive relief or other equitable relief."[102] However, the relevant way in which a plaintiff can establish "loss" under the CFAA in behavioral advertising cases is subject to a $5,000 threshold.[103] The plaintiffs bringing suit against advertisers have seriously struggled to meet this requirement and have had difficulties showing there was non-consent when they agreed to privacy agreements.[104]

The ECPA includes the Wiretap Act, the Stored Communications Act, and the Penn Register Act.[105] The ECPA's original purpose was to provide equitable relief to people whose electronic communications were "intercepted, disclosed, or used" during transmission of the communica-

97. Serwin, *supra* note 51, at 815. The FTC, it its most recent Report, again called upon Congress to consider legislation. *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, 26 (2012) available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

98. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e) (1984); Electronics Communications Privacy Act, 18 U.S.C. § 2510 (1986).

99. *Id.*

100. *See In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 519 (S.D.N.Y 2001); s*ee also Bose*, 2011 WL 4343517, at *10 (dismissing plaintiffs' claims under either theory for failure to meet minimum damages requirement of failing to show non-consent in both cases).

101. 18 U.S.C. § 1030(e).

102. *Id.*

103. *Bose*, 2011 WL 4343517, at *7.

104. *Id.* The other type of damages that could be shown are: "potential modification or impairment of a medical diagnosis, examination, treatment, or care of one or more persons, physical injury, a threat to public health or safety, or damage to a government computer that is used in furtherance of the administration of justice, national defense, or national security." *See* SERWIN, *supra* note 54, at 61.

105. SOLOVE & SCHWARTZ, *supra* note 56, at 36.

tion from one party to another.[106] Most plaintiffs have brought claims under the Wiretap Act specifically, which extended privacy protection to information on telephone lines.[107] These claims have been dismissed, as well, though there is no $5,000 threshold for them to meet.[108] The problem that plaintiffs face is similar to ones with the CFAA, in that a privacy agreement is usually used as evidence of consent.[109] There is also an issue as to whether information that was obtained from cookies, rather than "during transmission," would violate the Act.[110] Under one of the ECPA exceptions, consent by a "party to the communication" exempts either the user *or* the Internet Service Provider (ISP) from being liable for third party interceptions.[111]

3. *Issues Courts have with Plaintiffs' Claims*

While there are debates about whether or not government regulation or self-regulation should guide overall consumer protection, there still seems to be an issue as to whether there really are legitimate privacy concerns over one's browser history, which may or may not contain personal information.[112] Courts have dismissed plaintiffs' claims regarding their personal information being tracked regardless of any legal theory they bring litigation under.[113]

Two of the common law legal theories plaintiffs have sought relief under are trespass to chattels and unjust enrichment.[114] The elements needed to prove a traditional trespass to chattels claim in tort law are: (1) that one dispossesses the other of the chattel; (2) the chattel is impaired as to its condition, quality, or value; (3) the possessor is deprived of the use of the chattel for a substantial time; and (4) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[115] In *eBay, Inc. v. Bidder's Edge, Inc.*, the traditional trespass to chattels claim was extended to cases involving computers.[116] In these cases, a plaintiff can

106. Bosset, et al., *supra* note 14, at 4.

107. HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 66 (Infobase Publishing rev. ed. 2006).

108. *See generally* Electronics Communications Privacy Act, 18 U.S.C. § 2510 (1986).

109. HENDERSON, *supra* note 107, at 66.

110. *Id.*

111. *In re Doubleclick*, 154 F. Supp. 2d at 519. (emphasis added); s*ee also* HENDERSON, *supra* note 107, at 66 (noting other exceptions to the ECPA, including the "business use exception, which permits interceptions in the ordinary course of business, and the service provider exception," which states that certain acts are "incidental to rendering service").

112. *See* Hirsch, *supra* note 9, at 444.

113. HENDERSON, *supra* note 107, at 66.

114. *La Court*, 2011 WL 2473399, at *3.

115. RESTATEMENT (SECOND) OF TORTS § 217 (1977).

116. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1148, 1154-55 (C.D. Cal. 2007).

establish that a defendant trespassed if: (1) he intentionally and without authorization interfered with the plaintiff's possessory interest in a computer system, and (2) the defendant's unauthorized use proximately resulted in damage to the plaintiff.[117] However, courts have held plaintiffs to a high standard, often having to prove an actual economic or tangible harm.[118] This has been a problem with plaintiffs because of the difficulty assessing a monetary value to one's personal information, and the right to one's enjoyment of their property has been limited to a showing of actual damage to the computer's functionality.[119]

The other common law legal theory plaintiffs have tried to use, unjust enrichment, requires that: (1) the defendant was enriched; (2) at the plaintiff's expense; and (3) this benefit conferred upon the defendant was unjust.[120] These claims have also failed because plaintiffs have not been able to prove that their personal information conferred a benefit upon advertising companies in a way that is unjust to them.[121] These courts, as well as the FTC, have noted that this benefit is not unjust because consumers, besides receiving a benefit from targeted advertising, are also receiving a service from the websites they visit, and often at no cost.[122]

4. *Summary of Cases to be Analyzed*

This comment points out three specific cases that will demonstrate the issues plaintiffs have had in bringing suits regarding their private information being tracked. In *Bose v. Interclick*, plaintiff Bose brought suit against Interclick, an advertising network company, claiming that Interclick used flash cookies to back up deleted browser cookies.[123] The plaintiffs alleged that they deleted the browser cookies that were deposited on their hard drive by the defendant to prevent their browsing history from being tracked and stored.[124] However, after deleting the cookies, the defendant respawned the browser cookie via the flash cookie

117. *Id.* The elements are revised to reflect the unique circumstances of computer invasion, yet seem to require similar showing of damages as a tradition trespass to chattels claim would require. *Id*.

118. HENDERSON, *supra* note 107, at 66. A more tangible harm would include a showing of actual damage to one's computer. *See Bose*, 2011 WL 4343517, at *7.

119. *La Court*, 2011 WL 2473399, at *8.

120. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 (2011).

121. *Bose*, 2011 WL 4343517, at *25.

122. Interview by John Villfranco, *supra* note 29 (noting that most people would prefer to have advertisements directed toward them). At the same time, they receiving a service from their ISP or from the website they are visiting. *Id*.

123. *Bose*, 2011 WL 4343517, at *1. The plaintiff brought suit under several legal theories, including the CFAA, New York state law claims, and state common law claims.

124. *Id.* at *3.

without consent.[125] The defendant moved for a motion to dismiss for failure to state a claim or cognizable injury under the CFAA.[126] The court granted all of the defendant's motions to dismiss except for the New York General Business Law § 349 claim and the trespass to chattels claim, and only because they were sufficient to survive a motion to dismiss in that they "adequately pled a claim."[127] This meant the case could go on to trial because there were enough facts to possibly prove the claim.[128]

In *La Court v. Specific Media*, the plaintiffs were consolidated into one action, claiming that they set the security control on their computers to "block third-party cookies and/or periodically delete third-party cookies," yet each had the cookies respawned by a "flash cookie" by the defendant, an online third-party network.[129] These flash cookies, plaintiffs contended, were installed without their "notice of consent."[130] They sought relief under the CFAA, trespass to chattels, unjust enrichment, California's Invasion of Privacy Act, Computer Crime Law, Consumer Legal Remedies Act, and Unfair Competition state laws.[131] The court first noted that the California Invasion of Privacy Act claim that the plaintiffs raised was "arguably preempt[ed] by ECPA," that unjust enrichment cannot serve as an independent claim, and that the plaintiffs failed to allege any impairment at all to their computers with respect to the tort claim.[132] The motion to dismiss was granted on all claims.[133]

Lastly, in *In re DoubleClick Inc. Privacy Litigation*, the plaintiffs also argued that the defendant advertising company violated the CFAA and ECPA by depositing cookies onto their hard drives without authorization when plaintiffs accessed websites that were affiliated with the advertisers.[134] After a lengthy interpretation of both statutes to determine

125. *Id.*

126. *Id.* at *1.

127. *Id.*

128. *Id.* at *22. Plaintiff failed to allege any facts regarding these claims against most of the defendants. *Id*. Defendant Interclick's motion was denied, however, and plaintiff was allowed to at least continue on with the pleading. *Id*. It is yet to be determined the outcome of this though. *Id*. The plaintiffs' New York state law claim maintained that the defendants practice constituted a "deceptive business act" by misleading customers into thinking that their information was private when it actually allowed customers' information to be tracked. *Id*. at *18. The court determined that the plaintiffs pled enough facts to at least survive a motion to dismiss, and that a privacy violation could constitute injury for purposes of Section 349. *Id*. at *19.

129. *La Court*, 2011 WL 2473399, at *2.

130. *Id.*

131. *Id.* at *8.

132. *Id.* at *7, *8 (C.D. Cal. Apr. 18, 2011) (noting that because unjust enrichment cannot serve as an independent claim, it cannot serve as independent cause of action; there was further detailed analysis concerning the unjust enrichment claim in this specific case).

133. *Id.* at *9 (C.D. Cal. Apr. 18, 2011).

134. *In re Doubleclick*, 154 F. Supp. 2d at 503.

the applicability of the statutes to these types of suits, the court granted the defendants' motion to dismiss.[135] The court concluded that the defendants fell into the ECPA exceptions, that the plaintiffs would be subject to the CFAA $5,000 minimum damages requirement (though they did not meet it), and that ECPA did not extend to the use of cookies here because DoubleClick received authorization "with respect to a communication of or intended for that user."[136]

This comment will argue that courts and regulatory bodies are out of sync with one another, if not just for the fact that one is trying to protect consumers while the other is denying that any "harm" exists.[137] Courts reject common law approaches to issues that arise under targeted advertising, as well as legal theories that attempt to state a claim under other statutes with a specific cause of action.[138] Meanwhile, Congress has tried to approach privacy issues as though they are inherent in targeted advertising, while the FTC, not willing to decry behavioral advertising altogether, instead adopts an approach that embraces the benefits of it while affording protection to consumers.[139]

III. ANALYSIS

So what is it exactly that the FTC and Congress are trying to protect? If it is just about giving people a choice, courts have dismissed cases where people exercised their choice, only to have it overridden by respawning cookies.[140] But to the plaintiffs that have demanded redress, it is not innocuous at all that their information is being tracked and stored.[141]

In an April 2010 interview with the Director of the FTC Bureau of Consumer Protection, the interviewer noted that the director had previously suggested that "tangible harm-based models" might not be adequately addressing other types of harms that are not economically able to be redressed, such as a "consumer's dignity."[142] This suggests that there actually are other harms other than tangible ones, and therefore

135. *Id.* at 527.

136. *Id.* at 519.

137. Bosset, et al., *supra* note 14, at 3.

138. *Id.* at 4.

139. Brief for Respondents, *supra* note 17, at 9.

140. *La Court*, 2011 WL 2473399, at *3.

141. *Id.*

142. Interview by John Villfranco, *supra* note 29. Thus, previous FTC policies are consistent with how courts have addressed plaintiffs' claims in that they consistently deny that any relief is available unless there was an economic injury, which itself denied since either nominal interference with the computers or because one cannot assign a monetary figure to their personal information. *See In re Doubleclick*, 154 F. Supp. 2d at 525 and *La Court*, 2011 WL 2473399, at *9.

other types of relief may be required to protect such harms.[143] Furthermore, there is more than one solution that will provide consumer protection.[144] This section will analyze each solution and propose whether it should be adopted as the best way to protect consumers from potential harms, including ones not yet recognized by many courts.

A. Harms that Should be Recognized

Consumer harms have proven difficult to define.[145] It is hard to argue for protection when courts have dismissed plaintiff's claims, stating that they suffered no tangible harm.[146] Moreover, these harms must be weighed against the purported advantage of behavioral advertising, as well as what proposed solutions could do to prevent them.[147] However, this comment suggests that there are at least two harms that should be acknowledged and afforded relief.[148]

The first is consumer dignity and personal autonomy.[149] This is violated when personal choice is overridden by flash cookies that respawn deleted browser cookies.[150] Once the browser cookies have been removed, the consumer has expressed her decision to not be tracked or have targeted advertising directed toward her, regardless of any benefit she may receive from it.[151] This has been supported by the FTC, recognizing that notice and choice models can be unclear and the harms-based model has only applied to consumers that have "suffered an economic harm."[152] Though both of these models have proved to be somewhat unreliable, they do indicate that the FTC does appreciate the importance of a consumer being able to understand privacy policies and having the ability to choose whether to accept them.[153] There needs to be teeth to this though by having a model that adequately protects, not just acknowledges, this right.[154] This could lead to courts also taking this right seriously.[155]

---

143. Bosset, et al., *supra* note 14, at 4.

144. *See generally* Bosset, et al., *supra* note 14.

145. *See* Hirsch, *supra* note 9, at 444.

146. Bosset, et al., *supra* note 14, at 3.

147. Interview by John Villfranco, *supra* note 29.

148. *Id.*; *see also* Schmierer, *supra* note 7, at 42; *see also* Brill, *supra* note 4, at 8. These harms would be adequately protected with the proposals this comment puts forth. *See generally* Interview by John Villfranco, *supra* note 29.

149. Bond, *supra* note 20, at 137.

150. *Bose*, 2011 WL 4343517, at *3.

151. *Id.*

152. Interview by John Villfranco, *supra* note 29.

153. Serwin, *supra* note 51, at 815

154. Brill, *supra* note 4, at 43.

155. Bosset, et al., *supra* note 14, at 3.

The second harm that should be recognized has two elements that need to be acknowledged. The first requires acceptance that people provide much more than their public record type information on the Internet.[156] The second is that information is not just bounced back and forth in a digital realm, but can fall into the hands of unwanted, and unwarranted, third parties.[157] Some users search for information that could be highly embarrassing or sensitive information, including searches related to sexual, medical, religious, and political inquiries.[158] Some sites ask for social security numbers.[159] There is an argument that even public record information is sensitive because if it is intercepted by an actual person rather than remaining in some digital logarithm, this could potentially identify the user along with his private searches.[160] Moreover, this should be balanced with one's right to "free speech and association," and one should not be forced to refrain from making online inquiries out of fear of being tracked.[161]

The ability for one to relate every private detail of his life becomes a real harm when it falls into the hands of a third party.[162] This could lead to "identity theft, credit card fraud, cyber-stalking, [and] damaged credit."[163] The government also has been able to receive personal information about consumers from internet service providers (ISPs) without obtaining a warrant first.[164] Rather, government officials are able to subpoena a user's search history, as though it were a document owned by the ISP with no regard to the personal information in it.[165] This is significant because the Wiretap Act set up requirements for a search warrant in order for the government to intercept telephone communications.[166] However, this has not been extended to situations in which the communications, or personal information, is transmitted via an Internet

156. Stallworth, *supra* note 19, at 473.

157. *See* Hirsch, *supra* note 9, at 444.

158. Schedwin, *supra* note 12, at 712.

159. *See* Hirsch, *supra* note 9, at 446.

160. *Id.*

161. Schmierer, *supra* note 7, at 11.

162. *See* Hirsch, *supra* note 9, at 446 (citing an investigation done by journalists that were able to find out what a particular user's name was by piecing together her searches after claims my major search engines that they do not link users' searches with their identities). That is, though these companies may not themselves link them, it was proven easy to do by a third party regardless. *Id.*

163. Stallworth, *supra* note 19, at 473.

164. Schedwin, *supra* note 12, at 711.

165. Hirsch, *supra* note 9, at 446. Note that a paradox is created by those who propose government involvement in regulation while admitting government itself creates privacy issues. *Id.*

166. HENDERSON, *supra* note 107, at 66.

search.[167]

Thus far, while non-economic harms have been somewhat acknowledged in the academy, no successful policy or framework has adequately addressed these, and courts certainly have not recognized them as any type of harm.[168] However, once these harms are recognized, progress can be made toward actual privacy protection.[169] That said, a distinguishing point about these harms must be mentioned. The first harm regarding personal choice reflects a situation in which the consumer has expressly deleted browser cookies yet they were respawned; here, the type of information stored should be irrelevant to a court's inquiry into the plaintiff's harm.[170] However, the second harm can either be premised on wrongful interception by third parties or on the type of sensitive materials that were obtained.[171]

B. Common Law Theories

1. *Trespass to Chattels*

Traditional trespass to chattels claims have been extended to provide relief for a plaintiff whose computer was trespassed upon *i.e.* hacked without authorization.[172] This is significant because, while it is certainly a step toward allowing one to recover when there has been no physical trespass, like on to one's land, it could also represent a way for plaintiffs to recover when their personal information is stored even for targeted advertising purposes.[173] However, some courts have seemed unwilling to extend this legal theory to claims where one's public record type information has been stored.[174]

That said, in keeping with the tradition of the trespass to chattels claims, there is also something to be said about plaintiffs who are so concerned about their personal information being tracked that they must continuously delete browser cookies.[175] This certainly interferes with one's ability to enjoy his property for a "substantial amount of time."[176]

---

167. Tristram R. Fall, III, *Current Developments in Privacy and Security- Impact of Technology*, 82 Pa. B.A.Q. 139, 145 (2011).

168. Bosset, et al., *supra* note 14, at 3.

169. Brill, *supra* note 4, at 43.

170. Goldman, *supra* note 13.

171. Stallworth, *supra* note 19, at 478. This is to say that demographic information that is obtained could be rendered harmless and the focus of the harm would be on the wrongful interception. *Id*.

172. eBay, Inc., 100 F. Supp. 2d at 1154-55.

173. *Bose*, 2011 WL 4343517, at *23.

174. Goldman, *supra* note 13.

175. *La Court*, 2011 WL 2473399, at *2.

176. *Bose*, 2011 WL 4343517, at *23.

Furthermore, one's concern over his history should not be questioned.[177] This would be unfair for the plaintiff to prove the seriousness of his concern, as his fears are already actualized by the possibility of third parties intercepting his search histories without consent.[178]

In *La Court v. Specific Media*, the court determined that the plaintiffs did not allege any actual harm or malfunction of their computers after Specific Media installed flash cookies on the plaintiffs' computers in order to track their browser history for the purpose of behavioral advertising.[179] The court rejected the claim that being unable to delete cookies impaired the computer, and made it clear that there must be an actual intention or threat to impair to a "degree that would enable them to plead the elements of the tort."[180]

Other courts have determined that this degree of harm must be tangible or economic, as is required under some statutory causes of action.[181] The court in *Bose v. Interclick* determined that there would need to be some hard proof that the functionality of the plaintiff's computer had been affected *i.e.* that she was deprived of her enjoyment of her property, as is required from a traditional trespass to chattels claim.[182] The court noted that though the plaintiff failed to allege facts regarding the tort claim for most of the defendants, it did not grant the motion to dismiss, claiming that there was at least an adequate pleading of the claim.[183] This indicates that the court in *Bose* was at least willing to hear out issues regarding one's personal information being stored.[184]

The main problem plaintiffs have is that one cannot assess an economic value to his personal information.[185] Therefore, claiming an economic injury because a company has obtained such information is difficult when the courts require a similar injury as is required under the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act statutory claims.[186] This is unfortunate for plaintiffs because it effectively eliminates their ability to state a claim under multiple legal

177. *Id.*

178. *See* Hirsch, *supra* note 9, at 445.

179. *La Court*, 2011 WL 2473399, at *2.

180. *Id.* at *8.

181. Bosset, et al., *supra* note 14, at 4. The statutes that require a tangible or economic injury that courts have regularly seen are the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. *Id*.

182. *Bose*, 2011 WL 4343517, at *23. The court notes that "unsolicited emails 'deplete hard disk space, drain processing power, and adversely affect other systems resources." *Id*. at *23, *24. However, plaintiff failed to allege any such harm or that she was deprived of the enjoyment of her computer due to any of these factors. *Id*. at *24.

183. *Id.*

184. *Id.*

185. Bosset, et al., *supra* note 14, at 4.

186. *Id.*

theories, even if the statutes and common law claims have different elements.[187] The court in *Bose v. Interclick* at least entertained the idea that there are ways in which harm could be shown, but that the plaintiff in that case did not allege such facts.[188] Though this still would require a tangible harm, it is not as high of a standard.[189] This should be expanded to show harm against personal dignity when plaintiffs expressed that they did not want their browser history tracked, yet companies did so against consumer wishes.[190]

The unfortunate aspect of courts denying trespass to chattels claims is that it denies the privacy implications of a company ignoring a consumer's wishes by respawning undesired cookies on his computer.[191] This is a good legal theory for plaintiffs who are arguing that their personal dignity and right to choice were harmed.[192] Plaintiffs should also allege that they are deprived of the enjoyment of their computer when they are constantly deleting browser cookies to ensure that they are not being traced every minute they are on the web.[193] Though it may seem nominal, it may be a step in the right direction for courts to hear plaintiffs out that their choices are being taken away.[194]

Lastly, one may argue that a consumer should avoid certain websites if she does not want to be tracked. However, most consumers are not aware that flash cookies exist.[195] This legal theory best addresses a

187. *Id.* This is especially unfair since in modern trespass to chattels cases, a plaintiff does not need to show that there was actual damage to the chattel, rather, that they were merely deprived of their enjoyment of it. *See* § 217. Thus, the real hurdle plaintiffs should have is whether they were deprived of the use, or enjoyment, of their computer. *Id*. They should at least be able to argue that point, rather than have their claims melded together so that if they cannot prove one, they automatically cannot prove another without the court seriously looking at each element of each claim. *Id*.

188. *Bose*, 2011 WL 4343517, at *22.

189. *Id.*

190. Bond, *supra* note 20, at 138 (citing Ruth Gavinson, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 425 n.9 (1980)) (describing a framework in which privacy is "described as the control of personal information and physical access"). Personal autonomy is related to choice over the access of one's personal information located in one's browser history. *Id*.

191. Interview by John Villfranco, *supra* note 29. This is a corollary of the first harm this comment espouses that should be recognized. *Id*. The actual information stored should not necessarily be a consideration by the court simply because demographic information is deemed harmless. *Id*. One problem the trespass to chattels claim could face is that it does not adequately address the second harm this comment suggests should be recognized because an actual harm must occur before relief is available. § 217. However, once these claims are brought to court, the potential threat of information ending up in the wrong hands will be acknowledged, and the trespass to chattels claim could become more viable in other contexts, as well. *See* Stallworth, *supra* note 19, at 473.

192. *Id.*

193. *Id.*

194. *Bose*, 2011 WL 4343517, at *25.

195. Schmierer, *supra* note 7, at 14-15.

situation where a plaintiff actively chose to not be tracked, and was unaware that she was being tracked anyway by respawned browser cookies.[196]

2. *Unjust enrichment*

Plaintiffs have also tried obtaining relief via quasi-contract theory, arguing that because plaintiffs in good faith gave their personal information to websites, they should in return receive goods and services offered by those websites.[197] California courts have held that unjust enrichment, or quasi-contract theory, cannot be an "independent claim;" thus it does not have an independent cause of action.[198] That is, quasi-contract is a theory or principle that underlies other forms of relief, but is not itself a remedy, and therefore nothing is recoverable solely under the theory of unjust enrichment.[199] Because there is either no cause of action that can be afforded and plaintiffs have failed to allege that they did not receive any service from the defendant after providing personal information, unjust enrichment claims have been dismissed.[200]

This is one common law claim that courts have rightly dismissed, if not for the simple fact it is not an independent cause of action.[201] Although a benefit is certainly conferred upon a defendant, the second and third elements still must be proven – that it was at the expense of the plaintiff and that it would be unjust to retain this information.[202] Arguably, websites use people's personal information specifically to benefit those whom they obtain the information from, and simply because they are being benefited by it as well, it is not automatically unjust.[203] It must truly be unfair for the defendant to retain the information, which is hard to argue since, as the FTC recognizes, people who use the Internet themselves receive a benefit from their information being stored for pur-

196. Interview by John Villfranco, *supra* note 29.

197. *Bose*, 2011 WL 4343517, at *25. Arguably, in the context of targeted advertising, when a consumer's choice is effectively taken away, their privacy is invaded. Bond, *supra* note 20, at 142. A customer should not be expected to see which advertisers every single website hires to track information and deposit cookies on a hard drive, as they cannot be expected to stop visiting all sites that might engage in such advertising practices. *Id*. Once they actively choose to opt out of a tracking situation, their privacy is invaded once that unauthorized user respawns cookies for the purpose of tracking their information. *See* Nehf, *supra* note 66, at 1728 (questioning "should [data collection] be limited if it undermines. . .personal autonomy, or should we just accept that our lives are increasingly an open book?").

198. *La Court*, 2011 WL 2473399, at *9.

199. *Id.*

200. *Bose*, 2011 WL 4343517, at *25.

201. Bosset, et al., *supra* note 14, at 4; s*ee also La Court*, 2011 WL 2473399, at *9.

202. § 39.

203. Brill, *supra* note 4, at 7.

poses of behavioral advertising.[204] Ultimately, although consumers in these types of cases conferred a benefit upon a defendant, they themselves also received a benefit, such as free e-mail service.[205]

It is important to point out that although unjust enrichment claims should presumably fail because the plaintiff is receiving a benefit from the defendant, this should not diminish a trespass to chattels claim for two reasons.[206] First, the elements of each claim are different.[207] Even though it may seem unfair for a plaintiff to recover since he received a benefit from a free Internet service, trespass to chattels does not require that one receive such benefit.[208] The trespass to chattels claims should turn on whether a plaintiff deleted browser cookies, continued service with a website, and then ultimately was tracked via flash cookies.[209] However, if one continues to go to a website and enjoy its services, unjust enrichment should fail, even if just for a technical inability to satisfy one element.[210]

Second, there is an argument that the plaintiffs are receiving a benefit not just from a website's or company's service, but from targeted advertising, as well.[211] With a trespass to chattels claim, the plaintiff would not have to argue that he did not enjoy the benefit conferred upon

---

204. *Id.*

205. *In re Doubleclick*, 154 F. Supp. 2d at 525. The problem with plaintiffs' unjust enrichment claims is they are receiving a benefit via the services, which are often free, from the companies obtaining their information. Interview by John Villfranco, *supra* note 29. That is, it just does not satisfy all of the elements of an unjust enrichment claim. § 39. The reason why it should not be an issue in the trespass to chattels claim is that, as this article suggests, the tort law should be extended to cover plaintiffs that have expressly opposed companies tracking their information and storing it. Bosset, et al., *supra* note 14, at 4. The elements of trespass to chattels do not require a showing of a benefit conferred or that the plaintiffs did not in turn receive a benefit or compensation. § 217. So, even though the unjust enrichment claims cut against the fact that it should not be important for a plaintiff to establish an economic value on their personal information, that is only because the elements of the restitution claims are just not met and cannot be reasonably manipulated or extended to cover plaintiffs. § 39. A logical extension of existing trespass to chattels elements is reasonable here though because it does not require a showing that plaintiff received a benefit from defendant, it merely requires proof that defendant accessed one's computer without authorization. § 217.

206. Interview by John Villfranco, *supra* note 29.

207. *See* § 217 and § 39.

208. § 217.

209. *La Court*, 2011 WL 2473399, at *3. Showing that service was continued would not be an element of the claim, but would be useful in showing that a plaintiff was being tracked after deleting cookies on their computer and continued service with an ISP or a website thinking that they were not being tracked. *Id*.

210. § 39.

211. Indiviglio, *supra* note 2.

him by a website which tracked his information.[212] Rather, one should only have to show that he or she opted out of the tracking process, yet was tracked anyway through a company's use of flash cookies.[213]

C. Statutory Causes of Action

1. *The Computer Fraud and Abuse Act*

Even though the original purpose of the CFAA was directed at computer hacking, there is a logical extension of the statute for plaintiffs that have attempted to disable the cookies placed on their computer.[214] For example, the CFAA's criminal section sets forth that "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer . . . shall be punished."[215] Though this is the criminal language of the statute, it can easily be applied to the civil section since its purpose should be the same: to deter defendants from accessing another's computer without authorization.[216] That element is clearly met when a plaintiff can prove that she purposely removed cookies from her computer so her personal information would not be obtained and stored, yet websites continued to respawn cookies in direct opposition to what the plaintiff desired.[217] The only hurdle at this point would be damages.[218]

Under CFAA present causes of action, plaintiffs simply are not meeting the $5,000 threshold in order to obtain relief.[219] This problem stems from the fact that it is very difficult for plaintiffs to either show that the functionality of their computer was affected very much by the respawning of browser cookies, or that they are unable to assess an economic value to their personal information.[220] However, if privacy concerns really do exist surrounding targeted advertising and the retention of personal information, there must be a way for plaintiffs to obtain relief when they have made a choice to not have their information stored.[221] Assuming these concerns are valid, it is simply too much to ask a plain-

212. § 217. A result otherwise would be unfair to the plaintiffs, especially have having opted out of being tracked. *La Court*, 2011 WL 2473399, at *3.

213. *La Court*, 2011 WL 2473399, at *3. Again, this is not to include another element to the tort. *Id*. Rather, this would help establish that the plaintiff did opt out of being tracked. *Id*.

214. Bosset, et al., *supra* note 14, at 4.

215. *In re Doubleclick*, 154 F. Supp. 2d at 525.

216. Bosset, et al., *supra* note 14, at 4.

217. Schmierer, *supra* note 7, at 15.

218. *Id*.

219. Bosset, et al., *supra* note 14, at 4.

220. *In re Doubleclick*, 154 F. Supp. 2d at 520.

221. Schmierer, *supra* note 7, at 42.

tiff to meet that $5,000 threshold in these specific cases.[222] Furthermore, the defendants in *In re DoubleClick* admitted that they did not have authorization to access the plaintiffs' computers and conceded that the plaintiffs were protected under CFAA.[223] The only argument the defendants raised was that plaintiffs simply failed to meet the $5,000 threshold.[224] This seems to imply that, had the plaintiffs met the amount required, they would have had a solid case.[225] A defendant can admit that it did not have authorization to access a consumer's browser history, yet it is currently acceptable because there is not a purely economic loss to the plaintiffs.[226]

Courts have also not been sympathetic to plaintiffs that have signed or accepted privacy agreements, which means that plaintiffs have accepted the terms, and thus, consented to other parties obtaining and storing their personal information.[227] However, this should be weakened in cases where a plaintiff's intent is established by showing that he removed cookies from his hard drive specifically so his information would not be retained.[228] Courts should be open to allowing a factual determination as to whether the plaintiffs in these situations actually signed privacy agreements and then removed the cookies, or if they removed the cookies first when there was no actual agreement between the parties, or whether the agreement itself is even valid.[229] This would help establish what the plaintiffs' intentions were in protecting their personal information, and if their wishes were simply ignored.[230]

2. *The Electronic Communications Privacy Act*

Plaintiffs have also brought suit under Title I, the Wiretap Act, of

222. *In re Doubleclick*, 154 F. Supp. 2d at 520.

223. *Id.* It is unfortunate also that such a high amount of damages has to be met in order for plaintiffs to obtain relief, even though defendants could be held liable for the exact same conduct that merely resulted in more economic loss. *Id.* This is an extreme burden on plaintiffs, especially given that courts are not allowing plaintiffs to aggregate their claims. *Id*. at 523. There seems to be a paradox at this point with the law and what plaintiffs' injuries are: simply because plaintiffs cannot access an economic value to their demographic information, courts will not hold defendants liable even when they admit they accessed a computer without permission. *Id*. at 520. This is especially significant in the context of flash cookies because, in those cases, plaintiffs have expressly opted out of having their information stored and there is direct evidence that defendants obtained the information anyway. *La Court*, 2011 WL 2473399, at *3.

224. *In re Doubleclick*, 154 F. Supp. 2d at 520.

225. *Id.*

226. *Id.*

227. Nehf, *supra* note 66, at 1729.

228. *La Court*, 2011 WL 2473399, at *3.

229. Nehf, *supra* note 66, at 1732.

230. *La Court*, 2011 WL 2473399, at *3.

the Electronic Communications Privacy Act.[231] They assert that their ISP allowed advertisers to intercept user data to build large profiles that would be used to direct advertisements back to the users.[232] The problem is that most plaintiffs have been unable to establish that advertisement companies did not have authorization or were not exempt from the statute. However, the problem with the Act is in the language of the statute itself: "It shall not be unlawful under this chapter for a *person* not acting under color of law to intercept a wire, oral, or electronic communication or where *one* of the parties to the communication has given prior consent to such interception. . ."[233] Thus, the users do not have to consent in order for a third party to gain access, which seems fair when transparent and fair privacy policies are in place.[234] But, what if the policies are not so clear? This has been an issue the FTC has been trying to approach for years, and has gone through several frameworks to adequately address it.[235] There should at least be a consideration as to the quality of the policy before dismissing plaintiffs' claims under the ECPA.[236]

Furthermore, at least one of the two harms previously identified by this comment would not be adequately protected by the current ECPA, the harm to one's personal dignity.[237] Consumers should be presented with clear policy disclosures in order to make an informed decision whether they should proceed or not with a certain ISP.[238] This is very important in the context of flash cookies, where consumers often do not realize that cookies have respawned on their computer.[239] Plaintiffs have also rightly argued that flash cookies are not controlled by browsers, and thus flash cookies are not subject to browser privacy policies.[240] Further, the use of flash cookies is usually not even mentioned in privacy settings.[241] This means that although consumers have agreed to privacy disclosures, they are not being fully informed of the potential for their

231. Bosset, et al., *supra* note 14, at 4.

232. *Id.*

233. *In re Doubleclick*, 154 F. Supp. 2d at 519 (emphasis added). Though maybe a superficial reading, it is worth noting that "person" could be construed very narrowly and not apply to businesses or digital interceptions where a person technically has no contact with the communication. *Id*.

234. Stallworth, *supra* note 19, at 473.

235. *Id.*

236. Bosset, et al., *supra* note 14, at 4.

237. Interview by John Villfranco, *supra* note 29.

238. Anne Keaty, et al., *Can Internet Service Providers and Other Secondary Parties Be Held Liable for Deceptive Online Advertising?*, 58 BUS. LAW. 479, 495 (2002).

239. Schmierer, *supra* note 7, at 15.

240. Bosset, et al., *supra* note 14, at 3.

241. ASHKAN SOLDTANI ET. AL, FLASH COOKIES AND PRIVACY 1, 2 (2009), *available at* http://ssrn.com/abstract=1446862.

information to be tracked, even after they delete browser cookies.[242]

Again, the type of information, innocuous or not, should not really be an issue for this type of harm.[243] Consumers' privacy concerns should not be delegitimized by companies that claim they only use demographic information for a benefit to the consumer, who may not want the benefit to begin with.[244]

Furthermore, Congress is already considering adding a cause of action under the ECPA expressly for companies that obtain someone's personal information without consent.[245] This could be significant because the way courts are interpreting the statute now, it does not matter which party authorized the interception, especially if there was a privacy policy in place.[246] Thus, at this point, ECPA claims are being denied while Congress is considering amending it, while at the same time dismissing state law claims because the ECPA preempts it.[247] This is paradoxical because there is an indicator that Congress sees legitimate privacy concerns, yet the court in *La Court v. Specific Media* dismissed the plaintiffs' complaint, concluding that the "[state] statute's application to the conduct alleged . . . [was] far from obvious."[248]

3. *Statutory Section Conclusion*

Some courts have argued that these federal acts preempt similar state laws.[249] This means that plaintiffs will find it difficult to be afforded relief via their state's laws, effectively eliminating another route to recovery.[250] It is very likely that the first step may be to include causes of action under these statutes since several courts are requiring plaintiffs to allege a "tangible" injury in common law theories similar to what is already required under these statutes.[251] Once these statutes allow a cause of action that provides relief for plaintiffs whose personal information has been stored for targeted advertising uses, perhaps courts will then allow plaintiffs common law relief as well, since they can show an actual injury.[252] However, it seems counter-productive for a plaintiff to have to wait for one avenue of recovery to open up in order to

242. Schmierer, *supra* note 7, at 15.
243. *Bose*, 2011 WL 4343517, at *3.
244. Interview by John Villfranco, *supra* note 29.
245. Bosset, et al., *supra* note 14, at 4.
246. *Id*.
247. *Id.*
248. *La Court*, 2011 WL 2473399, at *8. Applying the state or federal statute would presumably produce the same non-result for plaintiffs in that case. *Id*.
249. Bosset, et al., *supra* note 14, at 4.
250. *Id.*
251. *In re Doubleclick*, 154 F. Supp. 2d at 520.
252. Bosset, et al., *supra* note 14, a 4.

obtain access to another.[253]

However, because legislation can be slow to achieve, it might, either out of necessity or out of chronology, be that courts recognize the FTC efforts to acknowledge other types of harms besides economic ones.[254] This might be the faster solution; however, CFAA and ECPA should at least be adjusted to include a cause of action for plaintiffs who have expressly chosen to have cookies deleted off their hard drive, only to have them recreated via flash cookies.[255] In *In re DoubleClick*, the plaintiffs simply could not establish that the use of cookies caused them any harm.[256] Either way, there is an issue when companies act under the guise of consumer choice, allowing consumers to think they are making a choice by deleting cookies, only to have that choice irrelevant by persistent flash cookies.[257]

D. Legislative and FTC efforts

1. *FTC*

The FTC has for the most part consistently relied on self-regulation approaches for businesses, which requires that they create their own regulatory policies for obtaining and storing a customer's browser history and personal information and then merely adhere to those policies.[258] The FTC however has set out a framework for which companies should use when making their self-regulations.[259] These goals consist of greater user control and transparency of user agreements, which would include making agreements clearer and easier to read, and allowing express consent by the consumer to allow the company to specifically use his data for behavioral advertising.[260] These goals promote consumer dignity be-

253. *Id.*

254. Charles W. Johnson, *How Our Laws Are Made*, http://thomas.loc.gov/home/holam.txt (last visited Nov. 13, 2011). There are several ways in which a bill may originate: by a member in the Senate (unless it is a bill raising revenue), the House, a constituent or the President can propose one. *Id*. They can be discussed and debate by committees and subcommittees, and both the House and the Senate have different procedures for voting on a bill. *Id*. This process includes many discussions, conferences, proposals for amendments, and several readings of the bill. *Id*. Ultimately, both must pass the bill before it goes to the President for approval. *Id*. Note that all of the differences the House and the Senate had about the bill must be reconciled and a unified version presented to the President. *Id*. Even then, the President may veto it and send it back to Congress along with his reasons for rejecting it. *Id*.

255. 18 U.S.C. § 1030(g).

256. *In re Doubleclick*, 154 F. Supp. 2d at 525.

257. *Id.*

258. Nehf, *supra* note 66, at 1730.

259. *Id*.

260. *Id.* This is itself another problem. *Id*. Studies suggest that people do not read the disclosures because they are lengthy or contain legalease that is difficult to wade through.

cause it allows the consumers to understand what they are reading and have the ability to make their own informed decisions whether to proceed or not.[261]

The FTC also encourages companies to only store information for as long as necessary to "fulfill legitimate business needs," ensure that the data collected is reasonable for those needs, and to adhere to the policies they set forth to the consumer even if they change the policies later.[262] The latter point is to help contribute to the transparency and ensuring consumers understand that the initial policy they agree to will be the one committed to.[263] This helps avoid information falling into the hands of unwanted third parties because information stored will be used for specific purposes and will not be retained indefinitely, which contributes to the privacy risks.[264] Also, privacy policies cannot be altered once entered into, so there cannot be deliberate sharing of information with a third party.[265] One may argue that these policies the FTC has set forth are not binding on any company, and if a company so chooses not to adopt these, the goals are with no effect without the force of law.[266]

That said, regulation still might not be necessary as the mere threat of adopting full on regulation would cause companies to take self-regulation more seriously and take the initiative to adopt those policies.[267] This is supported by situations in which the FTC has threatened litigation, and companies then choose self-regulation that comports with those policies set forth by the FTC.[268] These arguments suggest that legislation by Congress is unnecessary because the FTC has adopted an approach that is flexible with changing technology and has a corollary effect where companies comply simply out of fear that the FTC or Congress will take more regulatory approaches or from the threat of being sued.[269]

Id. Behavioral studies show that people make inferences about information they may be missing, which could lead to agreeing to a disclosure they might not have normally accepted. *Id*. Moreover, if information presented, though difficult to read, seems innocuous, people tend to assume there will be innocuous consequences resulting from accepting a privacy agreement. *Id.* There is an argument to be made that notice and choice models are not the best way to protect people because it is not a "substantive control." *See* Nehf, *supra* note 66, at 1740.

261. Brill, *supra* note 4, at 9.

262. Schedwin, *supra* note 12, at 724.

263. *Id*. at 711.

264. 263. Brill, *supra* note 4, at 9.

265. Schedwin, *supra* note 12, at 724. This does not include criminal interceptions; rather it refers to business mergers and third party advertisers. *Id*.

266. Schmierer, *supra* note 7, at 58.

267. *Id*.

268. *Id.*

269. *Id*.

By still abiding by a self-regulatory framework and the goals it promotes, the FTC has shifted in its approach concerning behavioral advertising from a notice and choice model to the privacy by design approach.[270] This still asks companies to design policies that they promise to abide by, yet acknowledges that other harms exist besides economic harms.[271] This is very significant in that it reflects courts' unwillingness to provide relief to plaintiffs that do not establish tangible or economic harms, yet is willing to make the first step in doing just that.[272]

Because it is very difficult for the law to adapt and anticipate changes in technology, this FTC framework is important because it recognizes that one must try to adapt with developing technology that keeps traditional notions of privacy at the forefront.[273] This is a good framework because it balances the FTC's goals without over-regulating the market.[274] Because this newer framework allows companies to consider what type of privacy protections they would like to offer at the forefront of creating their disclosure policies, it allows protections to consumer privacy to be a component of the competition amongst the markets.[275] This is also important because it could achieve a desired method that does not simply redress a plaintiff's claims, but prevents harms, of all types, from occurring at the outset of privacy agreements.[276] Further, privacy by design inherently requires that companies continuously confront privacy issues at every stage of development of their products.[277]

However, despite the fact that the FTC continues to promote the privacy by design framework and that companies are starting to abide by them, the FTC continues to call on Congress to enact legislation.[278] How-

---

270. *Id.* at 43.

271. *Id*.

272. *In re Doubleclick*, 154 F. Supp. 2d at 525. This is not to insinuate that courts are waiting on the FTC to take action or that they base judgments on whether the FTC recognizes what is a harm; rather, this is to show further that if the FTC can recognize certain harms besides economic ones, eventually this could lead to statutes with causes of action then eventually successful common law claims that allow plaintiffs a remedy. *Id*.

273. Serwin, *supra* note 51, at 815.

274. Brill, *supra* note 4, at 9.

275. *Id*. The other side to this is that businesses in the forefront of the market could eventually dominate and essentially develop a model framework themselves, which in turn would be anti-competitive. *Id*. However, legislation and regulation can be very slow to wait on, and since the law and technology is a unique field that is changing quickly, solutions that allow flexibility should be favored over hard and fast rules set in stone that do not allow change with development of newer technology. Interview by John Villfranco, *supra* note 29.

276. Serwin, *supra* note 51, at n. 14 (citing Solove, *supra* note 70, at 1242).

277. Federal Trade Commission, *supra* note 97, at vii.

278. *Id.* "The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The

ever, legislation would destroy the flexibility the framework allows by taking it out of the free-market context, which is better adept at finding innovative ways to adopt ever-changing technology that the companies understand better than Congress.[279] By not over-regulating, and by encouraging companies to use the privacy by design approach, it allows room for technological innovation.[280] Too much regulation could make it very difficult for plaintiffs to try their claims based on advanced technology that legislation or FTC regulation was unable to keep up with.[281] The law can be a tool for change, but it takes a long time to enact, and often struggles to keep up with future, or even current, issues in the technological arena.[282] Thus, while new businesses may have an advantage in being able to design their privacy models in a way that is quicker than forcing older businesses to update theirs, competition hopefully would create an incentive for the older businesses to keep up.[283] Furthermore, companies tend to change their privacy policies enough where the FTC has made it one of the goals of company self-regulation to abide by the disclosures they promise to uphold when consumers read the policies.[284] Arguably, a company going back to change its policy cuts against this FTC goal, but it also, and more importantly, requires companies to reconsider their disclosures in light of a new framework that is correctly adopted by the FTC.[285]

The current FTC privacy by design framework allows companies to still engage in self-regulation, and also achieves the goals of keeping information for as long as business purposes require and only retaining information specific to those purposes, all while encouraging competition

---

Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation." *Id*. at viii.

279. Schmierer, *supra* note 7, at 75.

280. *Id*.

281. PHILLIP E. AGRE & MARC ROTENBERG, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 213 (1998).

282. *Id.* The authors claim that privacy laws have been a success when their goals were narrowly tailored, but that another problem with privacy laws is that their "target keeps changing" and that the target is "too broad." *Id*. Though these are legitimate problems, it will always be easier to list off the problems and find ways the law has been effective in different ways for each of those problems *independently*. *Id*. However, the goal is to find a solution to all of the problems listed. *Id*. The authors note that a "rational and broadly applicable set of privacy principles may be beyond reach of the law of any single state or nationality." *Id*. This lack of satisfaction, one that asks for broad application but not a broad target, among most privacy laws begs the questions whether legislation is appropriate in the area of behavioral advertising. *Id*.

283. Brill, *supra* note 4, at 10.

284. Schedwin, *supra* note 12, at 724.

285. *Id*.

in the market for privacy protection.[286] It does this by allowing privacy policies to be adaptable for each company's interest and encouraging them to consider privacy issues earlier than the "notice and choice" models, which only serve to inform the consumer that his browser history will be tracked and the information stored.[287] This will also allow recognition that there could be other forms of harm besides one that an economic value can be assigned to.[288] Ultimately, this seems to remedy the two effects of the notice and choice and harms-based frameworks by asking for more transparency from the beginning while also allowing flexibility (as technology develops) and recognizing harm in the dignity of consumer choice.[289]

This is the preferred solution this comment adopts because it works with the free market and encourages adaptations to common law claims.[290] However, there is yet another way that plaintiffs could see relief, and that is via newly enacted legislation.

2. *"Do Not Track" Bill*

While part B of this comment suggests that an amendment to CFAA could be the beginning of plaintiffs seeing relief when they are subjected to targeted advertising, it was not without a warning. The fact that Congress is already considering statutory reform that would include a cause of action similar to what was proposed earlier in this comment demonstrates that it is difficult for legislation to adequately protect consumers in the technological market.[291] David Vladeck has said that "we are addressing technologies that are evolving so quickly that it would be . . . foolhardy to try to set rules in place knowing that two or three years later they would be rendered obsolete."[292]

---

286. Bond, *supra* note 20, at 142. Too much privacy may actually be counterproductive and stifle the ability of advertisers to deliver the benefit to consumers who choose to participate in targeted advertising. *Id*.

287. Serwin, *supra* note 51, at 815.

288. Schmierer, *supra* note 7, at 42.

289. *Id*. at 79.

290. *Id*. The idea is that because courts, proposed legislation, and the FTC are out of sync with one another, it will require somebody to make the first move in actually recognizing other types of harms consumers could experience besides tangible ones. *Id*. If the FTC recognizes these types of injuries, such as harm to dignity or personal autonomy, hopefully courts will extend the trespass to chattels claims to cover these injuries as well (eliminating choice means less protection of personal information, and thus, trespass). Bond, *supra* note 20, at 142. This will also, hopefully, eliminate the need to amend existing legislation or enact a new online privacy bill. Bosset, et al., *supra* note 14, at 4.

291. Bosset, et al., *supra* note 14, at 4.

292. Interview by John Villfranco, *supra* note 29. Though David Vladeck was answering for the FTC, this clearly applies to legislative efforts, as well, that would be relying on the FTC to enforce its regulations. *Id*.

Even recently proposed bills, such as the "Do Not Track" Act of 2011, attempts to address new privacy concerns over mobile devices.[293] Though arguably it is good that this bill includes a provision that prohibits unauthorized collection of personal information via mobile devices, it is still subject to the criticism that even it will fall behind the times.[294] FTC Director David Vladeck has suggested that mobile phones could supplant laptops, and this can only hold true for such hand held devices, as well.[295] The point is that it will always be difficult to anticipate newer technologies no matter how advanced we think we are.[296]

Proponents of government regulation claim that the best way to protect consumer privacy is by establishing specific rules that limit businesses' ability to collect, store, and distribute one's information.[297] However, this is exactly what the FTC hopes to promulgate through the privacy by design framework, which encourages companies to establish clear policies earlier rather than later, after the harm is already done.[298] The FTC framework also encourages innovation by not binding them to inexorable rules that do not allow protection for future technology.[299] Simply saying that "we . . . should let [consumers] opt out" does not automatically mean that legislation is the best tool to accomplish that goal, as this comment has set forth in previous sections.[300] Because the FTC has already put forth a guideline for companies to follow, legislation would arguably only be "[maintaining] the status quo," but without the flexibility of the FTC framework.[301]

Furthermore, the FTC has in the past asked Congress to pass legislation that would further require businesses to comply with the notice and choice model the FTC had previously adopted. However, Congress declined to do so and the FTC began encouraging other means to promote the notice and choice model, one being self-regulation.[302] This indicates that Congress is somewhat unreliable when it comes to regulation anyway, but that the FTC is still able to establish its own framework without a statutory force of law.[303] This also reflects the FTC's ability to adapt as it sees fit due to changes in technology or because of frameworks that prove unable to adequately protect consumers.[304]

293. S. 913.
294. Bosset, et al., *supra* note 14, at 4.
295. Interview by John Villfranco, *supra* note 29.
296. *Id.*
297. *See* Hirsch, *supra* note 9, at 452.
298. Schmierer, *supra* note 7, at 43; s*ee also* Vine, *supra* note 82.
299. Bosset, et al., *supra* note 14, at 4.
300. Vine, *supra* note 82.
301. Schmierer, *supra* note 7, at 76.
302. Serwin, *supra* note 51, at 842.
303. *Id.*
304. *Id.*

In the FTC's most recent report containing recommendations to businesses and policymakers concerning privacy, it again called for legislative action.[305] Congress may be listening this time, as several proposals for do-not-track legislation have emerged, yet their efforts may be at a standstill at this time.[306] Meanwhile, the FTC still embraced privacy by design and called upon companies to develop ways to embrace the goals it set forth in the report.[307] It seems that not only is Congress unreliable, but also its actions unnecessary, as companies such as Mozilla, Microsoft, and Apple have already developed the "latest versions of their browsers [that] permit consumers to instruct websites not to track their activities across websites."[308] Several privacy advocates claim, however, that self-regulation is not enough, and has fallen short so far.[309] However, the fact that some companies are already taking steps to protect privacy does not mean that every single company has to. Rather, businesses that show concerns for privacy may be setting the bar for market competitiveness for privacy protection. Legislation could impede market innovativeness, setting minimal standards that force every company to adopt, creating no incentive for better privacy protection.[310] Further, having specific, yet not necessarily required, goals set forth by the privacy by design approach, rather than express mandates or strict guidelines, allows companies to experiment with the best way to achieve those goals.[311] The FTC should continue to "call on companies" to promote privacy initiatives, thus putting the burden on them to *want* to protect consumer privacy.[312]

---

305. FEDERAL TRADE COMMISSION, *supra* note 97, at vii.

306. Juliana Gruenwald, *Ad Industry, Privacy Advocates Spar Over 'Do Not Track'*, NATIONAL JOURNAL (September 21, 2012), http://www.nationaljournal.com/tech/ad-industry-privacy-advocates-spar-over-do-not-track—20120921.

307. FEDERAL TRADE COMMISSION, *supra* note 97, at vii.

308. *Id.* The FTC recently stated that its "final report highlights initiatives undertaken by a number of companies to respond to the Commission's call for Do Not Track: Microsoft, Mozilla, Apple, Google, the online advertising industry through the Digital Advertising Alliance, and the World Wide Web Consortium, an international standard-setting body, have all taken significant steps forward." *See FTC Testifies on Efforts to Protect Consumer Privacy*, *supra* note 78.

309. *Id.*

310. Kevin J. O'Brien, *Privacy Advocates and Advertisers at Odds Over Web Tracking*, NY TIMES (Oct. 4, 2012) http://www.nytimes.com/2012/10/05/technology/privacy-advocates-and-advertisers-at-odds-over-webtracking.html?pagewanted=all&_r=0. Dan Jaffe, the executive vice president of the Association of National Advertisers, went further to say "if these various proposals limit this type of advertising, it will cut down on the amount of free information that consumers have on the Internet, create incentives for online companies to erect pay walls, and lead to more shotgun forms of advertising." *Id.*

311. Schmierer, *supra* note 7, at 76.

312. FEDERAL TRADE COMMISSION, *supra* note 97, at vii.

Ultimately, while anticipating these innovations can be somewhat done, as is shown by the FTC privacy by design framework, there is something to be said about the sluggishness of legislation.[313] It could create gaps between those who simply the bill could not get to fast enough to protect and those it does, only in time for a new shift in technology to occur.[314] Legislation that would use the FTC to enforce the bill would cut squarely against the FTC's ability to call upon companies to adopt different approaches more quickly and efficiently than Congress would be able to.[315] Congressional regulation should be avoided altogether if consumer choice really matters since the FTC is in a better position to adapt quickly to technology changes that affect consumer privacy.[316]

As this comment has explained, there are several ways in which a consumer could be protected.[317] However, some ways are more effective than others, yet the best solution is one that contains realistic goals when attempting to protect consumer privacy when technology develops very quickly.[318] It should be flexible, like the FTC privacy by design framework, with policies that anticipate innovation and reflect all the possibilities of different types of harms.[319] Once these are adequately protected, they would inherently be recognized as true harms, hopefully prompting courts to recognize them as such, as well.[320]

IV. CONCLUSION

Targeted advertising affects nearly every person who performs searches on the Internet, has a Facebook profile, or a Gmail account.[321] Browser cookies are used to track these inquiries that contain personal information such as social security numbers, names, addresses, or embarrassing searches, and store them in large databases for decades.[322] When a user deletes the cookies deposited on the hard drive, the cookies are oftentimes respawned by flash cookies.[323] This is accomplished unbeknownst to the user, without his consent, and oftentimes without being subject to browser privacy agreements.[324]

313. Johnson, *supra* note 254.
314. *Id.*
315. S. 913.
316. Schmierer, *supra* note 7, at 76.
317. *See generally* Bosset, et al., *supra* note 14.
318. Interview by John Villfranco, *supra* note 29.
319. Schedwin, *supra* note 12, at 729.
320. Bosset, et al., *supra* note 14, at 3.
321. Stallworth, *supra* note 19, at 470.
322. *Id.*
323. Bosset, et al., *supra* note 14, at 3.
324. *Id.* at 4.

However, the FTC has claimed that there are benefits of targeted advertising to both consumers and businesses, but has still sought to protect the former while allowing the latter to engage in its business practices.[325] Because there arguably is a mutual benefit, it is likely that targeted advertising itself will not be outright banned.[326] Therefore, it is necessary to find a solution that allows the practice to continue while allowing consumers to be protected while they reap this benefit.[327] However, the protection that consumers receive should address at least two harms, and hopefully courts will recognize them, as well: personal dignity and autonomy, and the potential for unwanted third parties to intercept one's private information without authorization.

Because consumers receive a benefit from targeted advertising, unjust enrichment claims for that simple fact should fail.[328] However, other common law claims should survive, such as trespass to chattels.[329] This will require courts to eventually recognize that other harms exist besides tangible ones.[330] Trespass to chattels claims should survive when plaintiffs have actively deleted cookies on their computer because they did not wish their history to be tracked, and were unaware that persistent flash cookies would respawn the deleted cookies.[331]

This comment also seeks to endorse the FTC privacy by design approach in the hopes that courts will one day recognize other harms and thereafter reassess common law claims with these new harms in mind.[332] However, if this does not happen first, the less embraced alternative proposal is that Congress could amend the CFAA or ECPA statutes. Relief should be given to plaintiffs that had flash cookies respawn their browser cookies because at that point there would be no authorization for a website to intercept this information.[333] The lastly proposed solution is not embraced at all because it relies on legislation and regulation that cannot keep up with technology, even if it tries to.[334] A real issue plaintiffs have at this point, as well, is that their harms need to be clearly defined. Academic works and the FTC have begun to address these potential harms, yet courts are still unwilling to see a true harm when no showing of economic damage can be shown.

---

325. Interview by John Villfranco, *supra* note 29.

326. Brill, *supra* note 4, at 7.

327. *Id*.

328. Brief for Respondents, *supra* note 17, at 9.

329. Bosset, et al., *supra* note 14, at 4.

330. *Id*.

331. *La Court*, 2011 WL 2473399, at *8.

332. *Id.*

333. *Id.*

334. Serwin, *supra* note 51, at 815.

Ultimately, this is a complex subject and there may not be one best proposal, especially in an area of the law that is constantly changing and developing, leaving the law struggling to keep up with it in order to protect ordinary people that engage in technology every day.[335] It could very well be that there is a statutory cause of action for plaintiffs if legislators feel it is appropriate. Perhaps the FTC, by adopting policies that acknowledge other types of injuries, will encourage courts to take a different approach to the common law claims plaintiffs are making. The point here is that while the latter is this article's preferred proposal, plaintiffs will continue to be denied relief until one of those two things happen.

Either way, people just feel wronged by behavioral advertising practices, and whether these feelings are unfounded may be irrelevant.[336] Perhaps this is the first step in changing the minds of courts while being able to continually adapt it to the needs of consumers who use the Internet and allow their personal information to be a part of it. As of now, there simply is not a remedy it seems for plaintiffs, and that could make a case that there simply is no harm to redress.[337] But as long as people are feeling that they are harmed, it is always worth investigating the source of their injury and attempting to rectify it.

335. Interview by John Villfranco, *supra* note 29.
336. Vine, *supra* note 82.
337. *Bose*, 2011 WL 4343517, at *3.