Hastings Communications and Entertainment Law Journal

Volume 36 | Number 2 Article 8

1-1-2014

Rethinking Online Privacy Litigation as Google Expands Use of Tracking: Giving Meaning to Our Online Browsing and the Federal Wiretap Act

Filip Babic

Rethinking Online Privacy Litigation as Google Expands Use of Tracking: Giving Meaning to Our Online Browsing and the Federal Wiretap Act

by FILIP BABIC*

I. Introduction

While there has been much talk of online privacy, and more broadly consumer protection, online tracking was not in the position to affect our offline lives until recently. Tracking in the past was associated with providing a more tailored online experience, characterized by personalized ads and faster loading times.[1] In an attempt to stop online tracking, many special interest groups have tried to characterize online tracking as an "injury" to consumers in order to litigate the issue.[2] Since a user is free to ignore these ads, which may only be of interest to the user based on

* University of California, Hastings College of the Law, J.D. Candidate, 2014.

1. *Talk of the Nation: Data Mining: Does Online Privacy Matter?* NATIONAL PUBLIC RADIO (Mar. 1, 2012), *available at* http://www.npr.org/2012/03/01/147741213/data-mining-does-online-privacy-matter.

2. Ian Ballon & Wendy Mantell, *Cloud Litigation: Suing over Data Privacy and Behavioral Advertising,* CENTURY CITY LAWYER (Sept. 2011), http://centurycitybar.com/newsletter template/Sept11/article2.htm.

browsing history, courts view online tracking as an "injury" that is de minimis,[3] and not the "sort of violation which typically is compensable."[4] However, as Google begins using a user's browsing history in more expansive ways—particularly making judgments about the user based on her search—it should become increasingly apparent that pervasive data mining is an "injury" to consumers which needs to be curtailed.

As of March 1, 2012, Google implemented new privacy policies that altered the "use of personal information obtained from users."[5] Instead of keeping personal information "about a user of a given Google service separate from information gathered from other Google services,"[6] the new policies "consolidate[d] user data from across its services and create[d] a single merged profile for each user."[7] This policy has the effect of creating a distinct and complex online profile for each user, from which Google makes significant inferences about the user's character.[8] While many theorists generally have had trouble finding legal remedies to pervasive online tracking,[9] Google has made it easier to fit data mining into existing privacy laws as these practices are becoming increasingly invasive.

This note will argue that these practices violate the Wiretap Act (the "Act") as amended by the Electronic Communication Privacy Act ("ECPA").[10] The Wiretap Act provides a cause of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[11] The Act, originally drafted to prevent eavesdropping on telephone conversations,[12] requires interception of the contents of communication and not merely the circumstances surrounding the communication.[13] As Google's practices have made it easier for users to characterize their searches as the "contents of communication," the Wiretap

3. *Id.*

4. *Id.*

5. Elec. Privacy Info. Ctr. v. FTC, 844 F. Supp. 2d 98, 101 (D.D.C. 2012) (citation omitted).

6. *Id.*

7. *Id.*

8. *See Talk of the Nation*, *supra* note 1.

9. *See* Joshua A.T. Fairfield, *"Do-Not-Track" as Contract*, 14 VAND. J. ENT. & TECH. L. 545 (2012) [hereinafter Fairfield, *Do-Not-Track*].

10. 18 U.S.C. §§ 2510–22 (2012).

11. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (citing 18 U.S.C. § 2511(1)).

12. *See* Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 2 J. HIGH TECH. L. 87, 88 (2003); *see also* Mitchell v. Forsyth, 472 U.S. 511, 539 (1985).

13. *iPhone*, 844 F. Supp. 2d at 1061.

Act has become a plausible cause of action for consumers who are "injured" by Google's appropriation of their personal information. The irony is apparent: The new ways in which Google uses an individual's search history has made it easier to apply online tracking to existing privacy statutes, statutes whose drafters could not have foreseen the existence of such technology.[14]

While this note does not argue that the Wiretap Act is an ideal cause of action and makes no attempt at gauging the probability of its success, it attempts to show that the Act can provide a potential cause of action in a changing internet landscape. This note will use the following fact pattern, based on actual Google practices, as a basis for discussing the expansiveness of online tracking: A user types "guitar" into the search field and hits enter; the user then applies for a credit card from the same computer; the user receives a lower credit limit on the credit card for which she applied as a result of her previous search for "guitar."[15] The reasoning behind the change in credit limit in response to the search for "guitar" is based on an empirical study, which showed that guitarists and musicians are less likely to pay back their debts and/or pay them on time than other segments of the population.[16] Hence, Google makes an inference about a user from their search in a way that exceeds the user's expectations of the effects of her search.[17] While she may be getting a banner ad for Guitar Center on the next website she visits, she is also unknowingly getting a lower credit limit and higher interest rate on her next credit card offer.[18]

Part II of this note will begin by presenting people's perceptions and views on both the practice and effects of online tracking. Part III will argue that the ECPA can provide a plausible remedy to the problem of online tracking. Finally in Part IV, the limitations and potential pitfalls of litigating against Google will be discussed.

14. For an extensive argument that the common law should be expanded to govern behavior in the virtual world, see Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 BERKELEY TECH. L.J. 55 (2012) [hereinafter Fairfield, *Mixed Reality*].

15. *See Talk of the Nation*, *supra* note 1.

16. *Id.*

17. *Id.*

18. *Id.*

II. What Is the Problem with Online Tracking Anyway?

A recent survey, conducted by researchers at the Berkeley Center for Law and Technology, found that a majority of Americans do not want their personal information collected surreptitiously online.[19] The survey indicates that a majority of internet users are not aware of how pervasive and expansive online tracking has become, with the majority believing that online tracking is limited to "purposes of serving tailored advertisements,"[20] and with one in five telling researchers that "they believed advertisers were not allowed to track people when they browsed medical sites."[21] While this note is limited to discussing Google's practice of creating an online profile of each user, surveys have shown that people have similar misconceptions regarding the use their private data by social networks like Facebook and Myspace.[22]

Tailoring advertisements to a particular user is possible by employing the technique of *online behavioral advertising* ("OBA"), which creates a profile for a specific user based on his or her online activities.[23] This advertising profile is extremely profitable to companies like Google, as recent studies suggest that Google makes as much as seven hundred dollars per user per year.[24] The use of data mining, not limited to marketing purposes, has gone largely unnoticed by consumers mainly because of the

19. Somini Sengupta, *Study Finds Broad Wariness Over Online Tracking*, N.Y. TIMES (Oct. 8, 2012), http://www.nytimes.com/2012/10/08/technology/most-americans-are-wary-of-being-tracked-online-study-says.html?_r=0 states that:

> Sixty percent [of participants] said they prefer regulation to 'prevent Web sites from collecting information' about them; [twenty] percent said such a tool should allow them to block Web sites from serving up ads; and [fourteen] percent said they would like it to 'prevent Web sites from tailoring advertisements' based on sites they had visited.

Id.

20. *Id.*

21. *Id.*

22. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, Proceedings of the Sixth Workshop on Privacy Enhancing Technologies 36 (2006), *available at* http://heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

23. BLASE UR, PEDRO G. LEON, LORRIE FAITH CRANOR, RICHARD SHAY & YANG WANG, SMART, USEFUL, SCARY, CREEPY: PERCEPTIONS OF ONLINE BEHAVIORAL ADVERTING (Privacy Enhancing Technologies Workshop 2006), *available at* https://www.cylab.cmu.edu/files/pdfs/tech_ reports/CMUCyLab12007.pdf [hereinafter BLASE].

24. Joe Mullin, *How Much Do Google and Facebook Profit from Your Data?*, ARS TECHNICA (Oct. 9, 2012), http://arstechnica.com/tech-policy/2012/10/how-much-do-google-and-facebook-profit-from-your-data/.

opt-out approach to privacy in the United States.[25] Furthermore, recent legal scholarship suggests that the U.S. legal system is ill-equipped to deal with the privacy issues arising from data mining practices and online behavioral surveillance.[26] With the dramatic and rapid pace of evolving technology,[27] the law appears lethargic in the face of change, leaving special interest groups and legal scholars scrambling for a legal remedy capable of addressing such an unparalleled issue.[28]

III. The Electronic Communication Privacy Act Should Provide Recourse to Consumers to Protect Against Expansive Use of Online Tracking.

This note argues that ECPA,[29] may be able to provide a remedy to consumers frustrated with the way in which Google uses their private information. While historically the Act has not been successful in curtailing pervasive online tracking,[30] as Google expands the way in which it uses browsing data beyond marketing, it should become increasingly plausible to argue that Google's online tracking practices violate the Act.

The Act provides a private cause of action against any person, or company who "intentionally intercepts, endeavors to intercept . . . any wire, oral, or electronic communication,"[31] or who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."[32] Up to this point, litigants have had trouble fitting data privacy violation claims into existing federal statutes because the Act requires that the actual "contents of a communication" be intercepted.[33] The Act limits "contents" to "information concerning the substance, purport, or meaning of that communication,"[34] and information pertaining to the identity of the author, like "names, addresses, and phone numbers of

25. Eric Johnson, Steven Bellman & Gerald Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 13 Marketing Letters 5–15 (2002), *available at* https://www8.gsb.columbia.edu/sites/decisionsciences/files/files/defaults_framing_and_privacy.pdf.

26. *See* Ballon & Mantell, *supra* note 2.

27. There seems to be an Orwellian fear that our online activities, or even our Facebook profiles, will one day be used by potential employers to judge our moral character.

28. *See generally* Fairfield, *Mixed Reality, supra* note 14.

29. 18 U.S.C. § 2510–22 (2012).

30. *See* Ballon & Mantell, *supra* note 2.

31. 18 U.S.C. § 2511(a).

32. 18 U.S.C. § 2511(d).

33. *See* Ballon & Mantell, *supra* note 2.

34. *Id.* (citing 18 U.S.C. § 2510(8) (2012)).

parties,"[35] does not fit this definition.[36] Accordingly, Google does not violate the Act when it collects data concerning only users' identities and activities, as this information is used primarily to determine the interests of a particular user for marketing purposes.[37]

This note argues that the manner and means in which Google has begun to use the consumer's online activity violates the Wiretap Act due to the fact that Google's tracking methodology gives "meaning" to simple searches.[38] Within this note, "meaning" is defined as "what the source or sender expresses, communicates, or conveys in their message to the observer or receiver, and what the receiver infers from the current context."[39] Thus, according to linguistics, there are two points at which a communication is given meaning:[40] At the sending stage (the user typing in 'guitar'), and at the receiving stage (the search is used by Google to make assumptions about the user).[41] While a user may not have intended to convey such meaning to Google, or to a third party, Google is nevertheless creating meaning at the receiving stage, often unbeknownst to the consumer.[42] It should be noted that the discrepancy between what a sender intends to communicate and what meaning the receiver assigns to the communication is not by any means novel; in fact, it is pervasive through all forms and mediums of expression and communication.[43] Thus, these simple searches can and should be characterized as "contents of the communication" for purposes of the Act.

A. *In re iPhone Application Litigation*: The Wiretap Act

In re iPhone Application Litigation[44] demonstrates why the Wiretap Act has not provided a remedy in the past while simultaneously opening the door to future litigation involving data privacy. In *iPhone*, Plaintiffs claimed that Defendants "violated their privacy rights by unlawfully allowing third party applications ("apps") that run on the iDevices to

35. *Id.* (citing Hill v. MCI WorldComm Commc'n, 120 F. Supp. 2d 1194, 1195–96 (S.D. Iowa 2000)).

36. *Id.* (citing Jessup-Morgan v. America Online, Inc. 20 F. Supp. 2d 1105, 1008 (E.D. Mich. 1998)).

37. *Id.*

38. *See Talk of the Nation*, *supra* note 1.

39. Nick Sanchez, *Communication Process*, NEW JERSEY INST. OF TECH., http://web.njit.edu /~lipuma/352comproc/ comproc.htm (last visited Mar. 12, 2014).

40. For an in-depth discussion on linguistic "meaning" see GEORGE LAKOFF, WOMEN, FIRE AND DANGEROUS THINGS (1987).

41. *Id.*

42. *See Talk of the Nation*, *supra* note 1.

43. *Id.* (Think language, art, etc.).

44. In re iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

collect and make use of, for commercial purposes, personal information without user consent or knowledge,"[45] even though the consumers consented to privacy agreements when they bought their iDevices and downloaded apps.[46] The apps collected Plaintiffs' "addresses and current whereabouts; the unique device identifier ("UDID") assigned to the iDevice; the user's gender, age, zip code and time zone; and app-specific information such as which functions Plaintiff performed on the app."[47] Although the court found that such information was not considered actual "contents of communication" for purposes of the Wiretap Act,[48] the case demonstrates the court's willingness to consider broadening the federal statute in order to include modern technologies not previously captured by the Act.[49]

Plaintiffs in *iPhone* asserted multiple causes of action, but the court's analysis of the Wiretap Act indicates that it remains a viable cause of action for users who can characterize their Google searches as actual "contents of communication."[50] The court explained that "content is limited to information the user intended to communicate, such as the words spoken in a phone call,"[51] and does not include geolocation data that is generated automatically without user intent.[52] The court emphasized that Plaintiffs failed to state a cause of action under the federal Wiretap Act because they alleged only interception of "automatically generated geolocation data."[53] Such data contains only information concerning the identity of the parties and the fact that the communication took place.[54] However, interception of the "substance, purport, or meaning of that communication" would fall under the Act.[55] While the *iPhone* holding has been the norm in online data privacy cases, as companies like Google begin to assign "substance, purport, and meaning"[56] to the information they receive from users, it should become easier to conceptualize the idea that the data intercepted by companies are actual "contents of communication."[57]

45. *Id.* at 1049.
46. *Id.*
47. *Id.* at 1050.
48. *Id.* at 1061–62.
49. That is this note's reading of the case at least.
50. *iPhone*, 844 F. Supp. 2d at 1061.
51. *Id.* (internal quotation marks omitted).
52. *Id.*
53. *Id.* at 1062.
54. *Id.*
55. *Id.*
56. *iPhone*, 844 F. Supp. 2d at 1061.
57. *See* Ballon & Mantell, *supra* note 2.

Applying the Wiretap Act to the facts introduced in Part I would likely lead to a different result because it is both easier to show the intent requirement on the part of the user and to characterize a user's searches as actual "content of communication" within *iPhone's* broad definition. When a Google user enters the word "guitar" into the search field, the user is telling Google that he or she is interested in a guitar. If the user clicks on a store's link, the user is telling Google that he or she is interested in purchasing a guitar, and consequently interested in actually playing the guitar. The user effectively tells Google, "I'm interested in the guitar, what do you know about it?" If any doubt exists as to whether the user had intended to convey this message, the doubt is eliminated after the user clicks the first link in the search results. Thus, potential plaintiffs can satisfy the intent requirement, as these searches are not "automatically generated geolocation data"[58] created by our personal property, but are meaningful words purposefully entered into the search bar.

Although users may know that online tracking is designed to determine a user's interest, Google takes the process one step further by making assumptions about a user's offline habits based on the search terms entered into the search field.[59] Even though users are becoming accustomed to tailored advertisements, they are not accustomed to having their credit card offers impacted.[60] Users assume that Google operates more like a machine than a person, blindly generating answers in response to requests; this view may be perpetuated as much by Google, as by users' expectations of what an online search engine does.[61] However, much like an individual party to a conversation, Google brings its own perceptions, ideas, and experiences to the "conversation." It makes assumptions and inferences, as well as categorizes people based on what they are "saying." Ultimately, the "conversation" is given meaning based on inferences drawn from the collective experiences, in this case empirical studies and statistics, of the receiving party.[62] Even though most users may not view their Google searches as "contents of communication," Google finds them both meaningful and valuable.[63] As a result, this note suggests that, as many similar legal concepts develop and evolve over time, the courts should look at the way the parties treat the

58. *Id.*

59. *See Talk of the Nation*, *supra* note 1. (As discussed above, many users are not aware of the fact that they are being tracked, nor are they aware of how their information is being used.).

60. *Id.*

61. *See supra* Part II (the extent to which Google is misleading users regarding the breadth and implementation of the personal data they collect is beyond the scope of this paper).

62. *See Talk of the Nation*, *supra* note 1.

63. *Id.*

communication in order to ascertain whether or not it is meaningful to either party. In this case, Google searches should be considered the "contents of communication," even if a user intends to convey information about him or herself that is far different than what Google receives.

B. The Common Law, Communication, and the Need for Expert Witnesses

While the court in *iPhone* notes that *content* is limited to things a user actually "intended to communicate,"[64] how a person communicates is hardly limited to words alone.[65] The discussion of libel in *Weller v. American Broadcasting Co., Inc.*[66] is indicative of California courts' willingness to expand common law definitions of "communication" in accord with developments in linguistics and cognitive science. In *Weller*, the California court recognized that "linguists are able to identify and explain how certain rhetorical devices or patterns of speech convey implicit meaning."[67] While section 45 of the California Civil Code[68] defines libel as "words" and "language,"[69] the court recognized that the meaning of the words should not be analyzed in a vacuum.[70]

According to *Weller*, "the context, juxtaposition of certain pieces of information, the choice of words, and the tone and inflection of the speakers, were likely to affect the viewer's understanding of what was being said expressly and implicitly."[71] Effectively, implicit and explicit meaning is conveyed at the sending end, and then interpreted by the listener at the receiving end. While the inclusion of testimony by a professor of linguistics in a libel suit may be viewed as progressive, section 801 of the California Evidence Code "does not require that the jury be wholly ignorant of the subject matter of the expert opinion in order to justify its admission."[72] Despite the fact that a typical juror listens and interprets what people say on a daily basis, the court allowed jurors to hear expert testimony regarding how they interpret language, and glean meaning from the circumstances surrounding the statement.[73]

64. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012).
65. *See Talk of the Nation*, *supra* note 1.
66. Weller v. Am. Broad. Co., Inc., 232 Cal. App. 3d 991, 1001 (Cal. Ct. App. 2010).
67. *Id.* at 1008.
68. CAL. CIV. CODE § 45 (2012).
69. *Id.*
70. *Weller*, 232 Cal. App. 3d at 1008.
71. *Id.*
72. *Id.* at 1007 (citation omitted) (citing CAL. EVID. CODE § 801 (1967)).
73. *Id.* at 1007–08.

While Google searches are undoubtedly a type of communication, the question remains whether or not these searches represent the "substance, purport, or meaning," of the communication in the eyes of the law. Even though the facts in *Weller* are much different than the fact pattern used for this note, the case is indicative of the California courts' willingness to hear expert testimony regarding how language is interpreted. While the libel statute may limit the tort to "words" "or language,"[74] the court recognized the need to broaden the statute in order to bring it closer in line with the reality of how people understand and give meaning to words and language.[75] In our case, a litigant would fare better with an expert telling the court how OBA works and what techniques are used to interpret a user's search. By giving the court a closer look into this process, the court may see that the process is analogous to how people find implicit meaning throughout all forms of communication, allowing for a higher probability of characterizing Google searches as the actual "contents of the communication."

C. The Interception Requirement

The Wiretap Act prohibits the "interception of wire, oral, or electronic communications."[76] While the "interception" requirement may be problematic under the fact pattern provided by this note, *iPhone* at least demonstrates that the courts may be willing to interpret "interception" broadly. For our Google recipient, *iPhone* suggests that a court would be hesistant to dismiss a claim based on this requirement. The exception to the Act provides that it is not "unlawful . . . for a person not acting under the color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception."[77] Under the Wiretap Act, "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[78] Even though the statute can be read broadly, courts have expressed concern about "the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications."[79] In order to narrow the application of the statute,

74. *Id.*
75. *Id.*
76. 18 U.S.C. § 2511(1)(a) (2012).
77. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (citing 18 U.S.C. § 2511(2)(d)).
78. In re Pharmatrak Inc., 329 F.3d 9, 21 (1st Cir. 2003) (citing 18 U.S.C. § 2510 (4) (2012)).
79. *Id.*

courts have adopted a real-time requirement which requires the interception to be simultaneous with the transmission,[80] a distinction that appears arbitrary and pointless. Thus, communication intercepted contemporaneously from transmissions could violate the Wiretap Act, while communication intercepted from storage, or from a hard drive, would only implicate the Stored Communications Act ("SCA").[81]

The First Circuit observed that this dichotomy cannot successfully "address current problems" regarding internet privacy.[82] The court states that "technology has, to some extent, overtaken language. Traveling the internet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously a linguistic but not a technological paradox."[83] In *iPhone,* Apple argued that since its operating system was designed to "access and transmit location data from the mobile device to Apple's servers," it must have been "the intended recipient of the location data from users' mobile devices,"[84] and therefore could not have intercepted the data.[85] The court was reluctant to accept this argument, finding that the intended communication was "between the users' iPhone and the Wi-Fi and cell phone towers, and Plaintiffs appeared to allege that Apple designed its operating system to intercept that communication and transmit the information to Apple's servers."[86] The court held that "Apple cannot manufacture a statutory exception through its own accused conduct,"[87] and that, as a result, the statutory exception does not apply.[88] Even though the users were on Apple iPhones, the court found that the users' information was being intercepted by Apple at the point where it reached the Wi-Fi and cell phone towers.[89]

The willingness by the court to accept this type of argument, which employs the technical aspects of the transmission, could allow Google users to formulate their own argument as to how and at what point in the transmission their data is being intercepted.[90] While a user may have

80. *Id.* at 22.

81. *Id.*; *see* 18 U.S.C. §§ 2701–12.

82. *Pharmatrak*, 329 F.3d at 21, 22.

83. *Id.* (citing United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003) (internal quotation marks omitted)).

84. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012).

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. This note makes no attempt at discovering the intricacies of the Online Behavioral Advertising ("OBA") technique, nor how this data is later shared with third parties.

intended to share his searches with Google servers, operating as the Wi-Fi or cell phone tower in this case, the user likely did not intend to share their communication with anyone or anything but the server, such as those portions of Google responsible for implementing OBA.[91] The user definitely did not intend to share this information with third parties like credit card companies or advertisers.[92] Again, this note is arguing that after *iPhone*, courts are becoming more receptive to arguments that utilize the functional aspects of technology—the way in which communication is received and transmitted—as the basis for satisfying the interception requirement. As long as a potential plaintiff can pinpoint the location at which his intended communication is being appropriated, by either a party or a particular technological process not representing the intended receiver of such communication, such arguments become plausible.

D. Privacy Policies and Terms of Use

While the main focus of this note is the application of the Wiretap Act to current data privacy litigation, an analysis of such application would be incomplete without a discussion of the effects of both privacy policies and terms of use on such claims. Even though the use of data mining is disclaimed in websites' privacy policies and terms of use, few consumers actually read these policies,[93] which have the effect of binding the consumer to the terms set forth in those agreements.[94] Privacy policies and terms of service ("TOS" also known as Terms of Use, or "TOU") may be deemed adhesion contracts, effectively telling consumers not to use the website if they do not like the terms.[95] As Professor Joshua Fairfield points out in his article *"Do-Not-Track" as Contract*,[96] consumers have no ability, aside from abstaining from using certain websites or the Internet altogether, to stop the use of online tracking.[97] "[C]ourts only look at corporate-drafted terms even when they are attempting to protect consumer interests, consumer victories are one-shot, flash-in-the-pan victories that merely

91. A discussion of the effects of Google's Privacy Policies and Terms of Use will be discussed in more detail below. *Infra* Part III.D.

92. *See Talk of the Nation*, *supra* note 1.

93. The author has not read these policies, which seems to be the norm among legal scholars. *See* Fairfield, *Do Not Track*, *supra* note 9, at 551.

94. *See Talk of the nation*, *supra* note 1.

95. *See* Fairfield, *Do Not Track*, *supra* note 9, at 545.

96. *Id.*

97. *Id.*

cause the corporation to rewrite its End User License Agreement ("EULA") or TOS to avoid the prior result in future cases."[98]

Despite Professor Fairfield's jaded view on privacy policies, recent case law suggests that perhaps these adhesion contracts are not fatal to data mining litigation.[99] *iPhone* suggests that courts are increasingly willing to take a discerning look at these contracts, and interpret ambiguities in favor of the plaintiff.[100] In *iPhone*, Apple claimed that the Plaintiffs' claims were foreclosed by the privacy policies and the terms and conditions of the iTunes Apps Store (the "Agreement"),[101] which "explicitly permitted" and disclaimed all liability "arising from third party conduct."[102] The court did not take this claim for granted and proceeded to take a discerning look at the policy, stating that "[i]f a contract is capable of two different reasonable interpretations, the contract is ambiguous."[103] The court went on to state that "[i]n cases of uncertainty not removed by the preceding rules, the language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist."[104]

To be clear, this note is not trying to assert that such ambiguity actually exists in the Google privacy policy,[105] only that this court was willing to take a discerning look at these policies in order to make sure they are valid in disclaiming all warranties. The court declined to rule on the validity of the Plaintiffs' claims at summary judgment, as "[p]laintiffs have a colorable argument that the terms of the privacy agreement were ambiguous and do not necessarily foreclose the remaining claims against Apple."[106] Interestingly, the ambiguity stemmed from what the court saw as competing definitions of "personal information" in the privacy policy. One clause stated that Apple "may collect non-personal information including zip code, area code, unique device identifier, [and] location,"[107] and can "collect, use, transfer, and disclose non-personal information for any purpose"[108] while Apple defined personal information in a separate

98. *Id.* at 580.

99. Similar to the intercept requirement discussed above, the court in *iPhone* appears hesitant to dismiss the claim based on the terms of use.

100. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1076 (N.D. Cal. 2012).

101. *Id.*

102. *Id.*

103. *Id.* (citing Oceanside 84, Ltd. v. Fid. Fed. Bank, 56 Cal. App. 4th 1441, 1448 (1997)).

104. *iPhone*, 844 F. Supp. 2d at 1076.

105. Due to the length of the typical privacy policy, one could presume that ambiguity does indeed exist.

106. *iPhone*, 844 F. Supp. 2d at 1076.

107. *Id.* at 1077.

108. *Id.*

section as "data that can be used to uniquely identify or contact a single person."[109] Such personal data cannot be as freely disclosed, used, collected, or transferred under the Agreement,[110] leaving both the consumer and court uncertain as to which provision applies to a user's geolocation data.

The court's finding of ambiguity in Apple's privacy policy illustrates the fact that such policies should not be perceived by potential claimants as absolute bars to any potential claims they may have. Despite the Plaintiffs' "colorable" argument concerning the user agreements, the court was reluctant to find for Apple, indicating that such claims have the potential to overcome any barriers established in the privacy policy.[111]

While a thorough discussion exceeds the scope of this note, it is worth mentioning that one problem that has been incipient upon Google's privacy policy is the online tracking of minors under the age of thirteen, who are legally not allowed to enter into contracts disclaiming their privacy rights.[112] At least among minors, Google cannot obtain permission to track.[113]

As online tracking and data mining practices evolve over time, views on potential privacy violations should also change. Both the courts and potential litigants should not limit themselves to Professor Fairfield's bifurcated view, which leaves consumers deciding between completely abstaining from using Google services, or accepting that their online activity will be subject to monitoring.[114] In *Branding Privacy,* a recent article recognizing the inadequacy of the opt-in/opt-out regime, Professor Paul Ohm sets forth a novel proposal that utilizes the signaling qualities of trademarks in order to "meet the notice deficiencies of privacy law."[115] He argues that any company dealing with customer information should be forced to "bind its brand name to a fully specified set of core privacy commitments."[116] This notion of "branding policy" is an example of an innovative solution to evolving privacy concerns which should not be dismissed merely because a website contains a link to an adhesion contract entitled "Privacy Policy." In balancing privacy concerns with theories of

109. *Id.*

110. *Id.*

111. *Id.*

112. *See generally* Andrea M. Matwyshyn, *Education Innovation and the Law: Generation C: Childhood, Code and Creativity,* 87 NOTRE DAME L. REV. 1979 (2012) (citing the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2006)).

113. *Id.*

114. *See Talk of the Nation, supra* note 1.

115. Paul Ohm, *Branding Privacy,* 97 MINN. L. REV. 907, 911 (2013).

116. *Id.* at 911–12.

free enterprise, the opt-in/opt-out system fails to properly apprise users of how their online activity is being utilized, and has thus proven to be defective.

E. Standing and the Injury-in-Fact Requirement

In order to satisfy the "case and controversy" requirement of Article III of the U.S. Constitution the plaintiff needs to allege: "(1) [I]njury-in-fact that is concrete and particularized, as well as actual and imminent; (2) wherein injury is fairly traceable to the challenged action of the defendant; and (3) it is likely (not merely speculative) that injury will be redressed by a favorable decision."[117] In *iPhone*, Plaintiffs' alleged "actual injury," which included "diminished and consumed iDevice resources, such as storage, battery life, and bandwidth."[118] Among the personal information collected by the iPhone apps were the Plaintiffs' "home and workplace locations, gender, age, zip code, terms search, Plaintiff's app ID and password for specific app accounts, etc., through each of the downloaded apps."[119]

While the court was reluctant to find standing based on these "injuries," the court found that "[t]he injury required by Article III may exist by virtue of statutes creating legal rights, the invasion of which creates standing."[120] This last statement is oddly circular because standing is a "threshold" question where an actual injury is required.[121] The logic of the statement is as follows: (1) Plaintiffs allege a violation of the Wiretap Act; (2) the Wiretap Act provides that "any person whose electronic communication is intercepted, disclosed, or intentionally used in violation of the Act may in a civil action recover from the entity which engaged in that violation;"[122] (3) if the court finds that plaintiffs have established a prima facie case under the Wiretap Act then the "alleged facts are sufficient to establish that they have suffered the injury required for standing under Article III."[123] Effectively, if plaintiffs can allege sufficient facts that the Wiretap Act was violated, plaintiffs can claim a concrete injury for the

117. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1053 (N.D. Cal. 2012) (citing Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2012)).

118. *Id.* at 1054.

119. *Id.*

120. *Id.* at 1055 (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975) (internal quoatation marks omitted).

121. *Id.* at 1053.

122. *Id.* at 1055 (citing 18 U.S.C. §§ 2510)(internal quotation marks omitted).

123. *iPhone*, 844 F. Supp. 2d at 1055 (citing Gaos v. Google, Inc., 2012 WL 1094646, at *3 (N.D. Cal. 2012)).

purposes of Article III standing.[124] Interestingly, many of the injuries alleged by the Plaintiffs in *iPhone* are not only injuries to their own sense of privacy, but injuries to their property—their iPhones—and their bandwidth. While discussion of effects on the use of cookies on computers is outside the scope of this note, after *iPhone*, pleading such injury will prove to be futile. Even though establishing a violation of the Wiretap Act will satisfy the injury requirements, there is no doubt that defendants will continue their attempts to dismiss these allegations before trial. Thus, in order to gain traction the fact pattern provided by this note[125] may be sufficient to show injury-in-fact, as the example provides an opportunity for litigants to conceptualize, and categorize such effects of online tracking as a distinct and palpable injury.[126] Hopefully, the courts' view of "injuries" to users stemming from online tracking as de minimis[127] will begin to change as users' begin to experience real effects from their online behavior.

F. Limitations on Litigation and Google's Ubiquity

One of the biggest problems for Google's users is that some consumers do not have a choice to opt-out, or to stop using Google altogether, since many employers require their employees to create a Gmail account as their primary work-email account.[128] Additionally, some users view online tracking and data mining as the cost of doing business.[129] Google provides a great service, but one that is not really "free."[130] Some argue that Google should be viewed as an exchange, where Google is able to "take user data, sell it to advertisers, and make money that allows them to give themselves a paycheck while keeping you afloat in free digital services."[131] While this may be true, the problem is that many users are not aware of the breadth and scope of the exchange and feel that their costs are limited to the banner ads they receive on subsequent websites for products they previously searched.[132] As the scope of online tracking broadens, it is important for the law to recognize and curtail these practices before their limitations

124. *Id.*

125. While this note bases its argument on the "guitar search/credit limit decrease" discussed in length above, there is no doubt that there are other such instances of online tracking that result in the negative impact on a users' offline life.

126. The effects being a lower credit limit.

127. *See* Ballong & Mantell, *supra* note 2.

128. *See Talk of the Nation*, *supra* note 1.

129. *See* BLASE, *supra* note 23.

130. *Id.*

131. *Id.*

132. *See* Sengupta, *supra* note 19.

become indiscernible and affect our offline lives in more distinct and tangible ways.

Another consideration is that Google is a powerful business tool, and many companies rely on Google to help them generate business and attract customers. Recently, French authorities attempted to have Google comply with their privacy policies; along with most European countries, France's system is an opt-in system requiring the consent of the user before the website can track and data mine the user's computer.[133] In response, Google threatened to exclude all French links from search results, which resulted in the French authorities backing down.[134] They recognized that if Google removed its links from the search results, it would have an adverse effect on businesses. Such actions demonstrate Google's power to protect its business model.

The tides in the United States may change, as the Federal Trade Commission ("FTC") has taken action against Google in regards to the way that they have handled their users' personal data.[135] Even though these actions resulted in a settlement of a "record breaking $22.5 million civil penalty," Google is not changing the way it handles personal data, as the profits resulting from private data collection likely outweigh the costs of litigation.[136] Despite the failure to curtail Google's personal data collection, the FTC has sent a message to the rest of the world, namely that the United States cares about internet privacy and personal data.

IV. Conclusion

The Wiretap Act may become an increasingly plausible cause of action against the collection of personal data by search engines. As collected information is characterized and given meaning, internet searches should be considered as the actual content of the communication, even under the current reading of the statute. As Google implements users' information, sells it to third parties, and begins to affect the offline lives of its users, it will be more and more difficult for it to protect itself solely by disclaimer, articulated in its terms of use and privacy policy. As technology grows, interpretations of old statutes must expand to accommodate our privacy interests.

133. Michiel Willems, *Google Threatens to Exclude French Links from Search Results*, SNL KAGAN MEDIA & COMMC'N REPORT (2012).

134. *Id.*

135. Francoise Gilbert, *FTC v. Google: Lessons Learned*, INTERNET LAW & STRATEGY (2012).

136. *Id.*

***