2015

Selling or Spying: The Legal Implications of Target Marketing Through Geolocation Technologies

Krystina DeLuca

SELLING OR SPYING: THE LEGAL IMPLICATIONS OF TARGET MARKETING THROUGH GEOLOCATION TECHNOLOGIES

Krystina DeLuca

I. INTRODUCTION

There is a rule in my Parents' house. One that I would venture to say is probably a rule in most homes, albeit it a dwindling one: "No cell phones at the dinner table". It is hard to believe that not so long ago, wireless mobile devices were used solely to make and receive phone calls, perhaps "text message" for the savvy cell phone user. Those simple devices have turned into something entirely different with the advent of the modern Smart Phone, dubbed the "third screen" behind the television and the personal computer.[1] As a society we have come to rely on our Smart Phones for everything, from finding directions to communicating our whereabouts with friends. These devices have become an essential body part – impossible and frightening to be without. Yet, as a result of this modern, wireless world, we are constantly sharing personal information, particularly that of our geographic location.

During the last decade, the exponential rise of social media and access to the Internet has caused users to reevaluate the importance of monitoring personal information disclosure. Particularly, questions of privacy and control over personal information have gained momentum as data collection through geolocation technologies have become heightened legal and national importance. However, while geolocation has become a bit of a buzz word, defining the technology and its potential legal ramifications has proven difficult. Nearly everyone who uses the Internet is affected by geolocation in some capacity, whether they know it or not. The technology is constantly working to allow Internet sites and mobile applications (Apps) to instantaneously identify a user's geographic location, and in some instances, use that information to classify an individual

[1] Dana B. Rosenfeld & Matthew P. Sullivan, "Legal Growing Pains in the Mobile App Market", *Metropolitan Corp. Couns.*, Sept. 1, 2011, http://www.metrocorpcounsel.com/pdf/2011/September/13.pdf .

and target market accordingly. Specifically for Smart Phone users, if you have not "opted out" of being tracked by every application that uses the technology, and to a certain extent even if you have, your device is tracking you.

There is a common question voiced, particularly by younger consumers who frequently utilize technology in their purchasing behaviors: Why does it matter that Companies collect geographic data, especially when the tools provide a benefit to the consumer? After all, most will agree the growth of Smart Phone devices and mobile Apps have provided interesting, seamless ways to connect social media with purchasing behaviors and shared activities. The answer: Money, power, and a serious invasion of personal privacy. As previously stated, Geolocation technologies can aggregate a comprehensive profile of a person through tracking a user's travel patterns, work habits, and precise location at any given moment. With this information, market actors gain an advantage to use or misuse this data without much concern of breaking any Federal law. Indisputably, this technology and its potential have begun to revolutionize internet commerce and communication; however, the law has failed to keep up with the technology, leaving both Companies and consumers unaware of potential legal ramifications that may arise.

This article seeks to address recent litigation regarding the use of client-side geolocation technologies, particularly in conjunction with the surge of Smart Phone devices available. Furthermore, it aims to provide a recommendation to Companies on how to best utilize the technology in order to prevent the legal ramifications that may arise. Part II will give a brief explanation of geolocation technology, address the rising presence of client-side geolocation tools through the use of Smart Phones, and speak to

the effect this has in target marketing campaigns. Part III will examine current case law to underscore how Courts, who generally side with Defendant Corporations, have begun to grant Plaintiffs a pass at the pleading stage, particularly on claims asserting violations of the Consumer Legal Remedies Act, Unfair Competition Law, and User Agreements. Part IV will discuss the Wiretap Act, a significant claim asserted where Plaintiffs have generally failed. It will also explore the ongoing California case *Joffe v. Google* and discuss how this could be a legal game changer for Plaintiffs asserting a Wiretap Act violation. Finally, Part IV will examine how a lack of action by the Federal Government, has prompted the Federal Trade Commission (FTC) and State legislatures to address privacy concerns and enforce safeguards against Companies utilizing the technology deceptively. Lastly, the article will provide three significant practices for Companies to consider before implementing geolocation technologies for target marketing purposes: Clear and concise User Agreements, opt-in functionality, and secure systems once personally identifiable information (PII) is collected.

II. GEOLOCATION TECHNOLOGY – WHAT IS IT?

In order to fully appreciate the impact geolocation has on the law, one must first understand how the technology, scarce until a mere few years ago, functions.[2] Generally speaking, geolocation is any means for detecting an Internet user's geographic location.[3] While the technology can serve many purposes, its appeal to the advertising industry began when companies saw its potential for target marketing to users in real-time based

[2] Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 Alb. L.J.Sci. & Tech., 61, 63 (2011).
[3] Martketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 Fordham, Intell. Prop. Media & Ent. L.J., 667, 592 (2012).

on their geographic location.[4] Though the technologies vary, most fall into two categories: client-side and server-side. Server-side geolocation technologies work remotely, acquiring information from a user that does not provide specific geographic location, but rather a user's Internet Protocol (IP) address.[5] The geolocation provider then evaluates the information against data contained in existing IP addresses and other geographic identifiers, matching an entry in the server's database enabler. When the geolocation provider makes a geographic match, it can often provide a website with a wealth of information about the user, such as the user's location within a twenty-five to fifty mile radius and the device used to access the site.[6]

Conversely, client-side geolocation tools operate on a user's personal computer or wireless device to automatically identify a user's location through a Global Positioning System (GPS) or nearby wireless tower. Once the user's location is tracked, the device will transmit that location when a website or content provider requests it.[7] This user-centric model enables client-side geolocation tools to more readily collect and disseminate personably identifiable information (PPI). Further, client-side technologies establish a closer nexus with the user since Smart Phones and other GPS-equipped devices can be located within a radius of a few dozen feet as opposed to server-side technologies that collect data regionally.[8] While client-side geolocation has been less

[4] *Id.* at 587.
[5] *Id.*
[6] King at 68.
[7] *Id.*
[8]Hiawatha Bray, "Software Puts Captions on the Real World", *Boston Globe*, Sept. 24, 2009, http://www.boston.com/business/technology/articles/2009/09/24/software_puts_captions_on_the_real_world.

common in the past, the widespread increase of GPS-enabled Smart Phones has made this technology progressively more popular and controversial.[9]

The most intuitive, and perhaps the greatest, use of geolocation technology is content localization through navigation Apps like Waze and mapping platforms such as Google Maps, Mapquest, and Bing Maps.[10] However, in surveying the geolocation landscape, Companies are progressively using the geographic data for target marketing purposes, prompting the "World Wide Web" encounter to become less worldwide.[11] As the technology develops, websites are increasingly blocking certain groups of users – curbing the Web to target a specific region or user group.[12] As an example, Digital Envoy, a leading geolocation provider, syndicates a user's location with census data to target ads based on demographic profiling. Data collection such as this allows companies to serve different ads to users of the same website. For instance, the site could target market a high-end "Gold" American Express card to a user connecting from a wealthy suburb while simultaneously recommending the standard "Green" card to a user from a less affluent area.[13]

Smart Phone Apps and other client-side tools are following suit as platforms like Google Now, Foursquare, and Yelp direct individuals with recommendations, reviews and deals based on the user's specific location.[14] The new features are designed to

---

[9] *See* Ryan Kim, "Apple's Boosts Smart-Phone Market Share", *S.F. Chron*., Feb. 24, 2010, at http://www.sfgate.com/business/article/Apple-s-boosts-smart-phone-market-share-3198940.php (recounting the increasing rate of Apple's iPhone sales).
[10] JD Lasica, "Beyond Foursquare: Geolocation Services Proliferate, Mature", Feb. 28, 2013, at http://www.pbs.org/idealab/2013/02/beyond-foursquare-geolocation-services-proliferate-mature058/.
[11] *Id.*
[12] Anick Jesdanun, "Geolocation tech slices, dices World Wide Web", *USA Today*, July 7, 2004, at http://usatoday30.usatoday.com/tech/news/2004-07-10-web-geolocation_x.htm#start
[13] *Id.*
[14] Lasica, supra note 10.

automatically present information to a user in real-time – even before you ask for it.[15] With an increase of these "targeted" applications, companies like Google and Apple have discovered more discreet methods of tracking users geographically and marketing accordingly. The personal nexus of client-side tools coupled with the increase of Smart Phone applications pose incredible opportunities for future commerce as well as potential privacy risks. Thus, this article will focus on client-side geolocation technology as privacy questions and issues appear to be outpacing the legal remedies available.

III. BRIEF HISTORY OF CASE LAW AND SUCCESSFUL CLAIMS

In lawsuits addressing geolocation issues, the Courts have struggled to uniformly apply the law[16], often attempting to fit old laws into new technologies. As with all novel claims, Plaintiffs tend to "throw in the kitchen sink" when filing complaints against Defendant Companies, hopeful their injury will fit into a state or federal statute. Contrary to popular consumer belief,[17] current federal law does not require Corporate giants like Google, Apple, and other App makers to obtain user consent, or even notify the user when collecting personal data through geolocation tools.[18] However, while Defendant

[15] *See* Mark Hackman, "Google Knows More About You Than Your Family Does – Are You Okay With That?" Jun. 29, 2012, at http://readwrite.com/2012/06/29/google-now-knows-more-about-you-than-your-family-does-are-you-ok-with-that (recounting how Google Now automatically creates a series of "cards" that try to assist a user by presenting information Google thinks you'll need real-time based on the personal data it's collected via how you use various Google services).
[16] *See* Somini Sengupta, "No U.S. Action, So States Move on Privacy Law, New York Times, (October 30, 2013), at http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?_r=0 (with no uniform Federal law in place, over two dozen privacy laws have been passed in more than 10 states in the year 2013).
[17] Joseph Turow et al., "Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It", (2009), at http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_ Advertising.
[18] Electronic Communications Privacy Act, 18 U.S.C §2702 (2006)

Companies have consistently been able to strike Plaintiff complaints with ease,[19] there are a few areas of the law where Courts are beginning to grant Plaintiffs a pass, at least at the pleading stage.[20] Part III will address the Consumer Legal Remedies Act, Unfair Competition Law, and Privacy Agreements, three areas of law where Courts are beginning to allow Plaintiffs to prevail. It's important to note that the 9th Circuit has taken the lead in addressing internet privacy issues;[21] and thus, CA State law and precedent cases will be the focus of this section. Furthermore, as mentioned previously, the law in this area is generally unchartered as Courts and State legislatures are beginning to recognize the impending privacy issues at stake. As a result, Part III will address recent litigation and analyze cases that are currently ongoing.

A. Consumer Legal Remedies Act

Due to the absence of federal precedent, plaintiffs will often invoke violations of State statutes or recently passed State privacy laws in lawsuits involving geolocation technologies.[22] With the vast majority of these cases occurring in California,[23] Plaintiffs have claimed a violation of the Consumer Legal Remedies Act under the California Civil Code.[24] The CLRA prohibits "unfair methods of competition and unfair or deceptive acts

[19] *See Yunker v. Pandora Media, Inc.*, No. 11-CV-3113-JSW, 2013 WL 1282980, at *13 (N.D. Cal. Mar. 26, 2013) (where Court denied Plaintiff's Wiretap Act, Stored Communications Act, CFFAA, UCL, CLRA, Breach of Privacy, Breach of Contact, Private Disclosure of Private Facts and Intrusion, Trespass, and Conversion claims with leave to amend).
[20] *In re iPhone Application Litig.*, 844 F. Supp. 2d. 1040 (2012); *See also In re Google Inc*., No.13-MD-02430-LHK, 2013 WL 5423918 at *24, (N.D. Cal. Sept. 26, 2013)(where Court denied Google's motion to dismiss Plaintiffs' Wiretap Act claims because Plaintiffs' sufficiently alleged Google exceeded scope of its own Privacy Policy and non-Gmail users did not consent to Google's interception of emails; however, the Court held Plaintiffs did not plausibly allege that they had an objectively reasonable expectation that their email communications were 'confidential' per Cal. Penal Code§623 nor did they sufficiently allege a Pennsylvania law claim as it related to those who receieved emails from Gmail users.)
[21] *See* Somini, supra note 16, (recounting that California, the long pioneer on digital privacy laws, has passed three online privacy bills this year).
[22] *Id.*
[23] *Id.*
[24] *iPhone II*, 844 F. Supp. 2d. 1040, 1069-71.

or practices."[25] A claim may be brought under the CLRA pursuant §1780(a) which provides any "consumer who suffers damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by §1770 may bring an action against such person".[26] The statute bans several types of conduct, such as representing that goods or services have characteristics or benefits which they do not have.[27] Further, the statute forbids entities from falsely representing that goods or services are of a particular standard, quality, or that goods are of a particular style or model.[28]

The CLRA is not a law of general application; rather, it applies to a narrow set of consumer transactions.[29] For example, a CLRA claim may only be alleged by a consumer, whom the CLRA defines as "an individual who seeks or acquires by purchase or lease, any goods for personal, family, or household purchases."[30] Consequently, the CLRA does not apply to government or commercial contracts nor does it apply to contracts formed by non-profit groups and other non-commercial organizations.[31] The CLRA is also inapplicable to customers entering into rental agreements.[32] Finally, while there is a jurisdictional split as to whether software is a good under the UCC,[33] the Ninth Circuit has previously determined the sale or licensing of software is not covered under the CLRA because software is neither a "good" nor "service".[34]

---

[25] Cal. Civ. Code §1770.
[26] Cal. Civ. Code §1780(a).
[27] Cal. Civ. Code, §1770(a)(5).
[28] Cal. Civ. Code §1770(a)(7).
[29] *Ting v. AT&T*, 319 F.3d 1126, 1148 (9th Cir. 2003).
[30] Cal. Civ. Code §1761(d).
[31] *See Cal. Grocers Assn. Inc. v. Bank of America*, 22 Cal. App. 4th 205, 217 (1994)(stating trade group, CGA, is not a consumer of services for family, household, or personal purposes as defined by the CLRA).
[32] *Lazar v. Hertz Corp.*, 143 Cal. App. 3d., 133, 143 (1983)(holding that a costumer who rented a car does not fall within the definition of a "consumer" under the CLRA).
[33] *Dealer Management Systems Inc. v. Design Automotive Group Inc*., 355 App. 3d. 416, 422 (2005)
[34] *See Ferrington v. McAfee*, No. 10-CV-01455, 2010 WL 3910169 at *19 (N.D. Cal. Oct. 5, 2010).

In the ongoing case *iPhone II*, Plaintiffs on behalf of both a Geolocation class and iDevice class allege that Defendant Apple violated the CLRA. Plaintiffs representing the Geolocation class claim that at a cost to the consumer, Defendant Apple stored geo-location information on user's iDevices for Apple's own benefit and Apple continued to collect geolocation data even when users switched the Location Services to "off".[35] They contend if Apple had disclosed the true cost of the geolocation technology, the value of the iPhone would have been materially less than what Plaintiffs paid.[36] Similarly, Plaintiffs representing the iDevice class argue that a significant reason for the purchase of their iDevice was the appeal of the alleged "free" Apps; therefore, had Apple disclosed its intentions to track and collect personal information via its applications, the value of the iDevices would be materially less than what Plaintiffs paid.[37] Furthermore, Plaintiffs hold that despite Apple's statements regarding privacy protection, Plaintiffs did not consent to Apple's tracking of their App use and personal information.[38] In both cases, the Court substantiated the CLRA claim, not because the Apps downloaded were deficient, but because the iDevices (a "good" under the CLRA) did not perform as promised by Apple to consumers.[39] Thus, Plaintiff's claim properly arose out of the sale of a good, not the downloading of software.[40]

[35] *iPhone II*, 844 F. Supp. 2d. 1040, 1070.
[36] *Id.*
[37] *Id.*
[38] *Id.* at 1071
[39] *Id.*
[40] *Id.*; *See also Yunker*, 2013 WL 1282980 at *13 (where Court denied CLRA claim by Plaintiff who downloaded Pandora App, finding that a number of districts hold downloading a "software" does not fall within the statutory definition of a good).

B. Unfair Competition Law

Plaintiffs litigating against Companies like Apple who utilize client-side geolocation tools may also succeed under their State's Unfair Competition Law.[41] The UCL creates a claim against business practices that are 1) unlawful, 2) unfair, or 3) fraudulent.[42] The law's coverage is sweeping and its standard for wrongful business is "intentionally broad" as to permit judicial tribunals to enjoin ongoing wrongful conduct as new business schemes, practices, and technologies continue to form and develop.[43] To assert a UCL claim, a Plaintiff needs to have "suffered injury in fact and…lost money or property as a result of unfair competition."[44] In other words, to establish standing under the UCL, a Plaintiff must show she personally lost money or property because of her reasonable and actual reliance on the alleged wrongful business practice.[45] Once injury is established, Plaintiff must show a statutory violation under one of the three prongs as each provides a distinct theory of liability.[46] Interestingly, Plaintiffs in *iPhone II* were able to prevail under all three prongs of the UCL, begging the question of whether Courts are starting to take a closer look at business practices exploiting geolocation technologies.[47]

Under the "unlawful" prong, the UCL prohibits any business practice that is also forbidden by law. Essentially, the UCL permits injured consumers to "borrow' violations of other laws and treat them as a separate, independently actionable claim of unfair

---

[41] *iPhone II*, 844 Supp. 2d, 1040, 1074.
[42] Cal. Bus. & Profs. Cody §17200.
[43] *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir. 2006); See also *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co*., 20 Cal. 4th 163, 180 (1999)("The Legislature ... intended by this sweeping language to permit tribunals to enjoin on-going wrongful business conduct in whatever context such activity might occur. Indeed, ... the section was intentionally framed in its broad, sweeping language, precisely to enable judicial tribunals to deal with the innumerable " 'new schemes which the fertility of man's invention would contrive").
[44] Cal. Bus. & Prof. Code §17204.
[45] *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 330 (2011).
[46] *Lozano v. AT&T Wireless Servs., Inc*. 504 F.3d 718, 731 (9th Cir. 2007).
[47] *iPhone II*, 844 F. Supp. 2d. at 1072-74.

competition.[48] Thus, in *iPhone II*, Plaintiffs were permitted to establish an independent action under the unlawful prong of the UCL through alleging Defendant's violation of the CLRA.[49]

Under the "unfair" prong, the UCL creates a cause of action for a business practice that is inherently "unfair", even if it is not be forbidden by law. For consumer cases specifically, the law under the unfair prong continues to be unsettled.[50] Some Appellate State Courts define "unfair" as prohibiting conduct that is immoral, unethical, or injurious to consumers and have applied a balancing test, weighing the benefit of Defendant's product or service against the gravity of harm to the alleged victims.[51] Conversely, other Courts define "unfair" per the UCL as conduct that violates public policy pursuant a specific statutory, constitutional, or regulatory provision.[52] In *iPhone II*, the Court did not apply one test over the other. Rather, the Court conceded that while the societal benefits of Apple's geolocation software may ultimately outweigh the harm to users, it was unwilling to make a factual determination at the pleading stage.[53] Other Courts have found this reasoning persuasive and substantiated a Plaintiffs injury without applying either balancing test for the "unfairness" of the geolocation service.[54]

Under the fraudulent prong, a Plaintiff must show that the public is likely to be deceived and allegations must be specific enough to give Defendants adequate notice of

---

[48] *CRST Van Expedited, Inc. v. Werner Enterprises*, Inc. 479 F3d. 1099, 1107 (9th Cir. 2007).
[49] 844 F. Supp. 2d. at 1072
[50] *Lozano*, 504 F.3d at 735-36 (California's unfair competition law, as it applies to consumer suits, is currently in flux)
[51] *S. Bay Chevorlet v. General Motors Acceptance, Corp*., 136 Cal. App.4th 1255, 1260-61 (concluding the test of an unfair business practice "involves an examination of that practice's impact on its alleged victim, balanced against the reasons, justifications and motives of the alleged wrongdoer…the court must weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim"; See also *People v. Casa Blanca Convalescent Homes, Inc. 159 Cal.App.3d*. 509, 530.
[52] *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co*., 20 Cal. 4th 163, 180 (1999).
[53] *iPhone II*, 844 Supp. 2d, 1040, 1073
[54] *In re Google Android Consumer Privacy Litig.*, No. 11-md-02264 JSW, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013)

the alleged misconduct.[55] Thus, claims of fraud must allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations."[56] Again, despite the specificity requirement of the statute, the *iPhone II* Court felt it was justified to allow Plaintiffs' claim to prevail. The Court found Plaintiffs on behalf of the geo-location class met the pleading burden through their allegations that in both Apple's Terms and Conditions and its letter to Congress, Apple ensured an opt-out option for the geo-tracking feature.[57] Plaintiffs showed they reasonably relied on Apple's representations that an opt-out feature was available when making purchasing decisions.[58] Similarly, Plaintiffs from the iDevice class successfully asserted that Apple's failure to disclose its collection of personal information through geo-location technology materially affected the value of the Apple device purchased.[59]

C. Violation of User Agreement

When deciding to grant a motion to dismiss, Courts have been allowed to consider "User Agreements" between business entities and users under the incorporation by reference doctrine.[60] Under California contract law, "if the language of the contract is clear and explicit, and does not involve any absurdity", then that language will govern the interpretation of the contract.[61] However, if the contract is capable of two different interpretations, the contract is ambiguous and the rules require the Court to interpret the

---

[55] *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir.1985).
[56] *Swartz v. KPMG LLP*, 476 F. 3d. 756, 764 (9th Cir. 2007).
[57] *iPhone II*, 844 F. Supp. 2d. 1040, 1074.
[58] *Id.*
[59] *Id.*
[60] *In re Gilead Scic. Sec. Litig.* 536 F.3d 1049, 1055 (9th Cir. 2008) (where Appellate Court reverses District Court's decision holding motion to dismiss was inappropriate when material representations by Gilead created an unrealistic positive assessment.)
[61] Cal. Civ. Code § 1638

ambiguity against the drafter.[62] While Plaintiffs have struggled to prove a violation of a User Agreement, particularly in the context of the internet, Courts are beginning to consider ambiguity in User and Privacy Agreements of tech giants like Google and Apple.[63] In *iPhone II*, the Court found Plaintiffs had a colorable argument that Apple's Privacy Agreement is ambiguous and found Plainiff's claims may not necessarily be foreclosed against Apple. The Court notes:

"It does appear that there is some ambiguity as to whether the information collected by Apple, including the user's unique device identifier, is personal information under the terms of the Agreement, and thus whether Apple's collection and use of the information is consistent with the Agreement's terms".[64]

Yet again, the *iPhone II* Court found that at the motion to dismiss stage, it was unwilling to rule Apple's agreement bars the company from liability.[65]

A California Court conducted a similar analysis of Google's Terms of Service and Privacy Agreements in *In re Google Inc.* Plaintiffs here challenged Google's operation of Gmail under the Wiretap Act alleging that Google intercepted, read, and acquired emails for the purpose of sending target advertisements relevant to the email sender, recipient, or both.[66] Looking closely at Google's policies, the Court found Google did not have implied or express consent to intercept emails to create user profiles and target market accordingly.[67] Furthermore, the Court noted that consent within Privacy Agreements may be express or implied. However, implied consent only applies to a narrow set of cases and the critical question is whether the parties whose communications were intercepted

[62] Cal. Civ. Code § 1654
[63] See *In re Google Inc. Gmail Litig*., 13-MD-02430-LHK, 2013WL 5423918, at *12-15 (N.D. Cal. Sept. 26, 2013); *iPhone II*, 844 F. Supp. 2d. at 1076
[64] *Id.*
[65] *Id.*
[66] *In re Google Inc.*, 2013 WL 5423918 at *12-15.
[67] *Id.*

had adequate notice.[68] Thus, the Court found it reasonable that Plaintiffs, upon reading Google's Privacy Policies, would not have necessarily understood that their emails would be intercepted for target advertisement purposes.[69]

IV. *JOFEE V. GOOGLE* – GAME CHANGER FOR THE WIRE TAP ACT?

The majority of Plaintiffs affected by geolocation technologies will focus their cause of action around a violation of the Wiretap Act. However, despite the frequency in which a violation of the Act is brought, Courts have consistently denied relief under the statute.[70] The Wiretap Act generally prohibits the interception of "wire, oral, or electronic communications".[71] Specifically, the Act provides a private right of action against a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[72] While Plaintiffs have failed to substantiate a Wiretap Act claim against Companies misusing geolocation technologies, a recent CA case may change the tide.[73]

In 2007, Google launched its "Street View" initiative, a panoramic viewing feature on its mapping services. To capture street-level images, Google mounted cameras

---

[68] *Id*.
[69] *Id.*
[70] *Id.* at 1062 (where the Court dismissed plaintiffs' Wiretap Act claim partly because geo-location data collected by Apple was generated automatically rather than *through the intent of the user*. Thus, the information did not constitute "content" prone to interception).; See also Google Gmail Privacy litigation, 2013 WL 5423918 NDCA 13-MD-02430-LHK (Sept. 26, 2013).
[71] 18 U.S.C. § 2520
[72] 18. U.S.C. §2511(1)(a)
[73] *Joffee v. Google, Inc.,* 729 F.3d. 1262, 2013 WL 4793247 (9th Cir. Sept. 10, 2013).

on a fleet of cars.[74] From 2007 to 2010 Google also furnished these cars with software and antennas capable of scanning wireless routers nearby to capture information like a network's name and whether that Wi-Fi network was encrypted or not.[75] This was done to enhance the accuracy of its location based services. However, the software also picked up actual data transmitted through the Wi-Fi networks. This "playload data" included emails, usernames, passwords, and other personal data.[76] In 2010, Google was highly criticized for the unwarranted data collection, publicly apologized, grounded the cars, and was ordered in some countries to delete the information entirely.[77]

Numerous class action lawsuits against Google eventually consolidated into the ongoing case *Joffe v. Google*. Plaintiffs ensued their cause of action claiming the Company's data collection scheme violated State and Federal wiretap laws.[78] In turn, Google moved to dismiss the case arguing the law was not violated because its data collection fell within an exception to the Wiretap Act per 18. U.S.C. §2511(2)(g)(i).[79] Under the exception, the interception of "electronic communication" that is "readily accessible to the general public" is permitted.[80] Two legal arguments flowed from the statutory exception. First, Google proposed the unencrypted Wi-Fi signal collected are a "radio communication" which by definition is "readily accessible to the general public". Second, Google argued that even if it wasn't a "radio communication" it was an

[74] Hanni Fakhoury, "What the Google Street View Means for Researchers (and Cops)", Electric Frontier Foundation, https://www.eff.org/deeplinks/2013/09/what-google-street-view-decision-means-researchers-and-cops, September 16th, 2013.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Joffe*, 729 F.3d. 1262 at 1263.
[79] *Id.*
[80] 18. U.S.C. §2511(2)(g)(i)

electronic communication that was “readily accessible to the general public” like a message posted to a public message board.[81]

Because the Wiretap Act does not specifically define what a “radio communication” means, the Court had to first resolve whether Wi-Fi signals are in fact what Congress intended to include under the exception.[82] Ultimately, the Court denied Google’s motion finding that unencrypted Wi-Fi signals were not "radio communications," but rather electronic communications.[83] The Court concluded that Congress meant a "radio communication" to mean a "predominantly auditory broadcast" like an AM/FM radio broadcast. Since the data sent over a Wi-Fi signal is not auditory, the Court held that it was not a "radio communication" under the Wiretap Act, regardless of whether a wireless access point used radio frequencies to communicate.[84] In determining that the "radio communication" exception did not apply, the Court also rejected Google's second argument that unencrypted Wi-Fi signals are "readily accessible to the general public."[85] The Court noted that unlike a radio station which could broadcast for miles, Wi-Fi signals are "geographically limited and fail to travel far beyond the walls of the home or office where the access point is located."[86] In addition, the Court reasoned Wi-Fi signals aren't "accessible" because capturing them "requires sophisticated hardware and software" and "most of the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network."[87] With this decision, the lawsuit against

[81] Joffe, 729 F.3d. 1262 at 1267-68.
[82] *Id.*
[83] *Id.*
[84] *Id.*; *See also United States v. Iverson*, 162 F.3d 1015, 1022 (9th Cir.1998) (“When a statute does not define a term, we generally interpret that term by employing the ordinary, contemporary, and common meaning of the words that Congress used”).
[85] *Joffe*, 729 F.3d. 1262 at 1277-78.
[86] *Id.*
[87] *Id.*

Google will continue, leaving the understanding and application of the Wiretap Act in a legal grey area.

V. WHAT COMPANIES UTILIZING GEOLOCATION TECHNOLOGIES SHOULD IMPLEMENTS

With the advent of geolocation technologies, the modern wired world has changed the way we interact considerably as the private sphere has become capable of new, seamless ways of tracking individuals.[88] Private companies can now effortlessly obtain electronic personal information that was once only preview to the government through an investigation.[89] As explained in Part II, geolocation technologies pose a considerable risk to individual privacy; and yet, Federal agencies have done little to address that risk.[90] With the absence of such laws, the Federal Trade Commission (FTC) has stepped in to address internet privacy issues, looking to Section 5 of the FTC Act and other rules governing online communities for guidance.[91] Section 5 empowers the Commission to restrain "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce".[92] Within those principles, the FTC has stressed heightened protection for "Personally Identifiable Information" (PPI).[93] In general, the Commission defines PPI as information that can be linked to a specific individual such as a name, postal address, email address, Social Security number, or driver license number.[94]

---

[88] Fred H. Cate & Robert Litan, Constitutional Issues in Information Privacy, 9 Mich. Telecomm. & Tech. L. Rev. 35, 61 (2002).
[89] *Id.*
[90] King at 115.
[91] *Id.*
[92] 15 U.S.C. §45(a)(1).
[93] King at 117.
[94] *Id.*

As noted previously, server-side geolocation technologies pose little risk to an invasion of PPI as they rely principally on IP-based and SSID-based identification techniques.[95] Server-side tools are not meant to identify a particular user; rather, these tools seek users regionally within a twenty-five to fifty-mile radius.[96] The same cannot be said for client-side geolocation tools. Again, the user-centric model allows for client-side technologies to more readily collect and disseminate PPI.[97] In recent litigation, Plaintiffs have claimed that Defendant Companies diminished the value of their mobile devices when the geolocation features collected plaintiff's PPI.[98] While the Ninth Circuit has yet to address the issue, District Courts have been reluctant to grant plaintiffs a claim *solely* based on the theory that the value of their PPI has been diminished.[99] However, when Plaintiffs bring forth other product harms, such as diminished battery capacity, overpayment theories, privacy issues and questionable user agreements, the Court has conducted a more thorough analysis of PPI collection.[100] Part V will address where Corporations have both succeeded and failed with their target marketing platforms through client-side geolocation and how the FTC has addressed them. Through this analysis, Part V will address the three critical practices Companies and web-site providers need to consider when utilizing geolocation platforms: 1) provide full discloser

[95] See Tedeschi, supra note 12 (explaining that geolocation mapping applications determine the location of the Internet service provider or server computer, not the exact location of the user)
[96] *Id.*
[97] *Supra* note 9.
[98] *In re Google, Inc.*, 2012 WL 6378343, at *4-6;*iPhone II*, 844 F.Supp.2d 1040, 1056; See also *Yunker* 2013 WL 1282980, at *3.
[99] *In re Google, Inc.*, 2012 WL 6378343, at *4–6 ; *Low v. Linkedin Corp.*, 2011 WL 5509848, at *4–5 (N.D.Cal. Nov.11, 2011); *See also iPhone II*, 844 F.Supp.2d 1040, 1054 ("Plaintiffs have alleged additional theories of harm beyond their theoretical allegations that personal information has independent economic value .").
[100] *Id.*

in User Agreements, 2) obtain user consent with regard to such practices, and 3) provide security of consumer information once it's collected.

A. Notice - Clear and Concise Terms and Conditions

Client-side geolocation technologies, which often pinpoint a person's location through a user's internet-connected device or Smart Phone, involve a thorough collection of PPI; thus, it is imperative that Companies provide significant notice with clear and concise terms before collecting such personal information. In the past, Companies have made the mistake of providing notice of data collection that is unclear, ambiguous, or buried deeply in excruciatingly wordy Terms and Agreement. The FTC has recommended that Congress enact legislation specifically to ensure a level of privacy protection by requiring websites and Internet companies to meet standards involving notice to consumers, consumer access to information, and security.[101] While Congress has yet to establish clear standards per this recommendation, the FTC has interceded in many cases where internet providers and website operators failed to follow their own privacy policies.[102] One noteworthy instance occurred when the FTC challenged Sear's practice of paying customers ten dollars to download software onto costumers' computers aimed to collect "research information" such as online purchases, bank statements, video rentals as well as the senders, recipients, and subjects of email messages. The issue was

[101] King at 117.

[102] *See* Sony BMG Music Entertainment; Analysis Proposed Consent Order to Aid Public Comment, 72 Fed. Reg. 13286, 13287 (Mar. 2007)(requiring Sony BMG to display prominent disclosure notifying customers that its products install software contain security vulnerabilities); Gateway Learning Corp., FTC File No. 0423047 (Sept. 10, 2004) (after promising to keep data private, company rented it to target marketers without customer consent); Microsoft, FTC File No. 012 3240 (Dec. 24, 2002) (publishing consent agreement after the FTC alleged that Microsoft's Passport feature collected personally identifiable information in excess of that described in its privacy policy); FTC v. ToySmart LLC, Civ. Action No. 00-11341-RGS (complaint filed July 10, 2000) (action for deceptive trade practices where defendant, now in bankruptcy, sought to sell its customer list notwithstanding promise in its privacy policy that it never would transfer customer information to third parties);

over Sears' disclosure agreement, which buried the tracking software's full capabilities in a lengthy and unclear document. The outcome ended in a settlement agreement where Sears' agreed to terminate collecting personal consumer information and destroy the data previously gathered.[103]

Open, honest disclosure of information is a critical solution to geolocation privacy issues and exactly the resolution the FTC and privacy advocates promote.[104] Clear notice will enable consumers to choose the appropriate level of privacy for them and whether the benefit of the product or service is worth foregoing their privacy.[105] In order for consumers to make an informed decision, Companies must provide them with clear, comprehensible information. Ironically, one of the biggest offenders, Google, has traditionally placed disclosure as a top priority.[106] In fact, many in the industry would attribute Google's success to two important corporate themes: "Be Honest" and "Be Open".[107] In fact, Google has often lead the way in undertaking measures and making concessions that other Companies have been unwilling to make.[108] Google's open model and willingness to admit to its mistakes has propelled the company to dominate practically every niche it has chosen to enter. Yet, despite the success the search engine

---

[103] *See* http://ftc.gov/opa/2009/06/sears.shtm (June 4, 2009).
[104] See Fed. Trade Comm'n, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 45-47 (2009), http:// www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter Self-Regulatory Principles.
[105] See Sony BMG Music Entertainment; Analysis of Proposed Consent Order to Aid Public Comment, 72 Fed. Reg. 13286, 13287 (Mar. 21 2007)(requiring respondent, Sony BMG, to display a prominent disclosure notifying customers that its products install software that create security vulnerabilities
[106] Jeff Jarvis, What Would Google Do?: Reverse-Engineering the Fastest Growing Company in the History of the World 95-98 (2009), *see at* http://aszapla.files.wordpress.com/2011/12/what-would-google-do.pdf
[107] *Id.*
[108] See Cyrus Farivar, "Google Bends to European Privacy Worries with WiFi Opt-Out Plan", *Deutsche Welle* (Sept. 14, 2011), at http://www.dw.de/google-bends-to-european-privacy-worries-with-wifi-opt-out-plan/a-15387075; Kevin J. O'Brien, "Google Offers More Privacy to Avert Clash with E.U.", *Int'l Herald Trib*. (Sept. 14, 2011), at http://www.highbeam.com/doc/1P1-197631044.html (discussing Google's efforts to avoid potential liability for privacy intrusion within the European Union).

King has reaped from its open approach, Google has made small steps toward implementing broad policies of disclosure in the realm of geolocation. To be fair to Google's efforts, it has created the program "Dashboard" which enables a user to manage the personal data associated with a user's account.[109] However, there is still much progress to be made by Companies like Google utilizing and it is highly recommended that these entities recognize that open disclosure is the key to consumer confidence.

B. Opt – In Agreement

Another way for Companies to protect themselves is to gain user consent by providing an "opt in" function to data collection rather than an "opt-out". If done properly, heightened consumer privacy would be ensured by holding Companies accountable for requesting user permission while ensuring that Companies request permission for geolocation data collection each time they desired it. While FTC regulations require that sites obtain user's consent before collecting personal data and geographic location[110], Companies do not always follow suit.[111] For instance, in fall 2012, Nordstroms implemented in-store technology that followed Wi-Fi signals of customers' Smart Phones to track the customer's movements throughout the store. The Wi-Fi tracking in conjunction with video surveillance enabled the clothing retailer to learn information about its shoppers such as age, sex, time spent in a particular aisle or department before purchasing merchandise, how frequently shoppers visited the store, and other demographic information. [112] Needless to say, once costumers caught wind of

[109] Privacy Tools, Google.com, http://www.google.com/privacy/tools.html (last visited Dec. 14, 2013).
[110] King at 122.
[111] Sam Lewis, "Nordstrom Experiment Highlights Privacy Issue", http://www.retailsolutionsonline.com/doc/nordstrom-experiment-highlights-privacy-issue-0001, July 18, 2013.
[112] *Id*.

Nordstroms' experiment, they were outraged and felt the testing without consent was a serious invasion of privacy. Subsequently, Nordstroms was forced to end its in-store research and destroyed the data previously collected.[113] Understandably, this type of personal data enables Retailers to better merchandize product to give the consumer a more efficient trip; however, it is imperative to give the consumer the choice to opt-in rather than make the decision for her.

Two recent examples show how the opt-in solution works in practice. In 2009, Google launched its My Location feature for personal computers which used SSIS-based and client-side geolocation tools to provide "more accurate local search results on Google third party sites.[114] During the product launch, Google sent an automatic prompt message explaining the My Location feature to all users equipped with Google's in-browser tool bar. The message also asked for the user's consent to install the application, and only upon the user choosing to opt-in would the product begin to collect and report geolocation data through My Location.[115] In August 2010, Facebook used a similar opt-in strategy when launching "Facebook Places", a feature that allowed users to share their whereabouts with friends through Facebook directly or through other third party platforms.[116] The notice and consent based model was a result of the Social Media company's development effort to put a stronger emphasis on user privacy than it had with previous Facebook features, which drew heavy criticism from the Electronic Frontier Foundation and other privacy watchdogs.[117]

---

[113] *Id.*
[114] King at 118.
[115] *Id.*
[116] Nick Bilton, "Facebook Will Allow Users to Share Location, N.Y. Times Bits Blog", Mar. 9th, 2010, at http:// bits.blogs.nytimes.com/2010/03/09/facebook-will-allow-users-to-share-location/.
[117] *Id.*

C. Adequate Security of Consumer information once collected

The third concern of the geolocation technology is ensuring adequate safeguards to keep the personal data safe once collected. Though corporate giants like Google and Apple claim they take the greatest precautions in securing data, two recent breaches of the Sony PlayStation 3 system have unmasked some scary realities.[118] In April and October of 2011, criminal hackers successfully accessed online subscriber information including the credit card numbers of seventy-seven million costumers.[119] The events proved that despite heightened security measures, even megacorporations like Sony may be unable to keep personal information secure. Thus, it is imperative that entities housing this personal data are certain the more secure safeguards are in place.

Foursquare, a location-based social networking App, is another company that has been under fire for faulty security of consumer information. Foursquare is an application that allows users to "check in" to venues such as restaurants, shops, and perhaps most frightening, an individual's home.[120] In February 2010, the site 'Please Rob Me' was launched to raise awareness regarding the thoughtlessness of location sharing. The site automatically scans data from public Twitter feeds that had been pushed from Foursquare to compile a list of people who are not home. The premise, while putting a humorous spin on it, is that since the user is not home, you can go rob them. According to the site's

[118] Charles Arthur & Keith Stuart, PlayStation Network Users Fear Identity Theft after Major Data Leak, Guardian, Apr. 27, 2011, http://www.guardian.co.uk/technology/2011/apr/27/playstation-users-identity-theft-data-leak.
[119] *Id.*
[120] Caroline McCarthy, "The dark side of geo: PleaseRobMe.com", *CNET.com*, Feb. 17, 2010.

founder, “On one end we're leaving lights on when we're going on a holiday, and on the other we're telling everybody on the internet we're not home." [121]

Later in 2010, white hat hacker Jesper Anderson exposed vulnerabilities on Foursquare that raised significant privacy concerns.[122] Foursquare’s location page displays a grid of fifty randomly chosen pictures of users who “checked in” to a location, regardless of the users’ privacy settings. So, whenever users “checks in” to a venue, their picture is generated on that location’s page, even if they only want their friends to know the location. Anderson was able to fashion a script that collected check-in information and successfully collected 875,000 check-ins.[123] Anderson then contacted Foursquare regarding the vulnerability and the social networking site changed its’ privacy settings to allow users to opt-out of being listed on the location page.[124] In 2012, Foursquare announced a change in its Application Programming Interface (API) for increase privacy. The modification was in response to a number of so-called “stalker” applications, like “Girls Around Me” and “Nock Nock” that rely on the user geographic data Foursquare provides to display a list of people filtered by gender who checked in nearby.[125] Again, as we become more connected, Companies cannot be ignorant to the security risks that come with the geolocation territory.

---

[121] *Id.*
[122] Singal, Ryan (2010-06-16). "White Hat Uses Foursquare Privacy Hole to Capture 875K Check-Ins". *Wired News*. Jun. 6th, 2012, http://www.wired.com/threatlevel/2010/06/foursquare-privacy/.
[123] *Id.*
[124] *Id.*
[125] Thompson, Chris. "Foursquare alters API to eliminate apps like Girls Around Me", May 10th, 2012, *see at* http://aboutfoursquare.com/foursquare-api-change-girls-around-me/

VI. CONCLUSION

Though geolocation capabilities were unheard of less than a decade ago, the developing technology offers accurate real-time means for identifying a user's geographic location. Companies and consumers are increasingly latching on to these tools – recognizing the wide range of benefits and efficiencies they can offer through target marketing and social media platforms. However, while the market has reacted quickly to the developing technology, the law has failed to keep up, leaving both buyer and seller in the dark. The ongoing march of technological advances is not only a good thing, it's essential to the economic and social revolutions of our time. However, as companies begin to utilize the technology in new and interesting ways, safeguards must be in place. The infringement of personal privacy by geolocation technologies is a serious problem that beckons a solution. More and more companies are utilizing the technology to target market their services or selling that data to third parties unbeknownst to the user. With a lack of uniform laws to protect personal information, the consumer is largely unaware of the transaction occurring, to whom that data may be benefitting, and who may be able to purchase the information.

At the end of the day, consumer privacy is critical to maintain and the Federal Government must take action to protect it. However, until that day comes, it will be up the FTC and States to implement privacy policies and hold Companies accountable for deceptively tracking personal information. Likewise, for the sake of good social policy, Companies utilizing geolocation should look to provide users with notice in clear User and Privacy Agreements, allow for a user to opt-in to the technology, and ensure the most secure practices to keep personal information safe. Disclosure is key and Companies

must be honest and open to instill consumer confidence. Geolocation tools will continue to develop and the "Googles" of the world will always be on the cutting edge of it as they should. Still, it's imperative that Corporations act responsibly; consumers continue to ask the important privacy questions; and for the Court system to keep up with the rapidly changing technology and establish new precedent to guide our modern world.