NOTE

GEOLOCATION AND TARGETED ADVERTISING: MAKING THE CASE FOR HEIGHTENED PROTECTIONS TO ADDRESS GROWING PRIVACY CONCERNS

RYAN MURA

It likely has happened to you before. You start by shopping online, but eventually choose to just visit the mall yourself. After looking through several stores without any success, you decide not to make a purchase and instead check back in a few weeks. However, for the next few days, any time you visit Google you see advertisements of the exact items you had considered buying from various online retailers. You also find these advertisements appearing on your Facebook newsfeed and Twitter timeline. You even receive emails from several local retailers advertising these same products. Feeling unsettled, you are left confused as to how retailers could possibly have information about your shopping interests.

The situation described is a classic example of marketers using geolocation services and other personal information for targeted advertising. While some consider it a mild annoyance and nothing more, studies have indicated that the vast majority of Americans are opposed to targeted advertising, particularly where geolocation is used to pinpoint a certain audience. Studies also reflect that Americans at large are misinformed about the current law governing geolocation services, and would in fact be underwhelmed with the lack of protections against information abuse. Therefore, given the growing concern with the collection, use, and dissemination of geolocational information for targeted advertising, current law should be adapted to require heightened notice and consent before providers can use geolocation, and the tort of intrusion on seclusion should be a remedy available for injured plaintiffs.

Analysis of this issue will proceed in three parts. Part I will discuss the history of geolocation services and the dangers of using geolocation for targeted advertising. Part II will survey the current law in this area and address its shortcomings, including the proposed Geolocational Privacy and Surveillance Act ("GPS Act"). Finally, Part III will explain the need for a different approach to geolocational privacy, including requiring affirmative consent and allowing injured plaintiffs to pursue damages under the tort of intrusion on seclusion.

I. HISTORY OF GEOLOCATION SERVICES

Geolocation is "the ability to locate individuals or objects using satellite technology."[1] This technology allows the provider to identify an Internet user's physical location by relying on their IP address.[2] More specifically:

> As the access-seeker enters the appropriate Uniform Resource Locator ("URL") into his/her browser, or clicks on the appropriate hyperlink, an access-request is sent to the server operating the requested Web site. As the server receives the access-request, it, in turn, sends a location request (i.e., forwards the access-seeker's Internet Protocol ("IP") address) to the provider of the geo-location service. The provider of the geo-location service has gathered information about the IP addresses in use, and built up a database of geo-location information. Based on the information in this database, the provider of the geo-location service gives the Web site server an educated guess as to the access-seeker's location. Armed with this information, the Web server can provide the access-seeker with the information deemed suitable. . . .[3]

Experts have estimated accuracy rates of IP-based geolocation services "between 85 and 98 percent at the state level and over 99 percent on the national level."[4] Some geolocation providers have claimed the ability to locate people "within feet" of their actual physical location.[5]

People use geolocation for several purposes. According to a survey conducted by a research company, the majority of respondents (41 percent) indicated that they use geolocation for "connection to other people I know or could meet."[6] The other most frequent responses were "finding a place liked by people I trust" (21 percent) and "insight about my travel or movement patterns over time" (17 percent).[7] Although these purposes seem

---

[1] Brent Dean, *The Dangers of Geolocation*, 8 Quinlan, Computer Crime and Technology in Law Enforcement 3, 4 (2012).

[2] *See* Kevin F. King, *Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 Colum. Sci. & Tech. L. Rev. 41, 58 (2010).

[3] Dan Jerker B. Svantesson, *Geo-location Technologies and Other Means of Placing Borders on the 'Borderless' Internet*, 23 J. Marshall J. Computer & Info. L. 101, 110 (2004).

[4] King, *supra* note 2, at 59.

[5] Nick Lane, *Mobile Geo-location Advertising will be a Big Number in 2015*, MobileSQUARED (March 2012), http://adfonic.com/wp-content/uploads/2012/03/geo-location-white-paper.pdf.

[6] Will Reese & Jamie Becklanda, *Lost in Geolocation: Why Consumers Haven't Bought it and how Marketers Can Fix it*, Mobile Marketing Report (Spring 2011), http://www.thelbma.com/files/59-Lost%20in%20Geolocation%20Report(1).pdf.

[7] *See id*.

noble and innocent, the potential for manipulation of the information collected is unsettling.

Geolocation services are prevalent not only in traditional web browsers, but also in mobile web browsers and smartphone applications that people use daily, including Facebook, Twitter, and Four Square. In fact, using certain smartphone applications allows the provider to use geolocation to make "a comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[8] For example, "disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[9]

Smartphones have become increasingly pervasive in our daily lives. Experts have suggested that there are 322 million wireless devices in use in the United States, and have estimated that 65 percent of the United States population will have a smartphone or tablet by 2015.[10] Indeed, "[a]s smartphones become ubiquitous, as people share more and more information voluntarily, and as more advanced monitoring techniques become possible, individuals may indeed lose any expectation of privacy they once had in their location."[11] Although the choice to share one's location may be voluntary, it's often made without a true understanding of the consequences. "Facebook invites users to share their location (and sometimes their friends' locations, too); foursquare handles millions of check-ins per day; and few of the technology-savvy, if any, are surprised when someone seems to know, without asking, where they have been that day."[12]

Providers use geolocation for much different reasons than consumers. Perhaps the largest and most utilized function of geolocation services is to present targeted advertising. Over the past decade, there has been a gradual decline in traditional, mass advertising.[13] Thus, "as there are fewer and fewer 'views' or 'listens' to particular advertisements, marketers remaining in the advertising market must increasingly personalize their advertisements

---

[8] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[9] People v. Weaver, 12 N.Y.3d 433, 441-42 (N.Y. 2009).

[10] Monica Mark, *GPS Tracking, Smartphones, and the Inadequacy of Jones and Katz*, Crim. Just. 36, 37,Winter 2013.

[11] *Id.*

[12] *Id.*

[13] *See* Timothy J. Van Hal, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for A Class Action Regime for Privacy Protection*, 15 Vand. J. Ent. & Tech. L. 713, 722 (2013).

to remain lucrative."[14] Marketers prefer targeted advertising because this practice "helps them deliver their persuasive messages to audiences who are most likely to be interested."[15] Moreover, this technology creates "the possibility of price differentiation in different markets or localized advertising,"[16] meaning retailers can adjust the price of an item based on its popularity in a certain market. Using geolocation for this purpose is valuable for advertisers because it allows the company to set a price that would maximize its profits.

Marketers have defended tailored advertising by asserting that Americans prefer ads that are specific to their interests and desires. One executive in the advertising field noted that "[s]omething amazing happens when marketing efforts are actually relevant to people. We see this step as initiating that crucial dialogue. And shoppers, for their part, are replying; essentially giving their permission to marketers to learn their habits and respond accordingly."[17] Google followed suit, and vaguely described its reasoning for using targeted advertising as "[i]t's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful."[18] Other proponents suggest that targeted advertising "helps support the providing of free content on the web . . . [and] it can reduce the time a user spends searching on the web."[19]

Contrary to marketers' beliefs, however, studies have indicated that the majority of Americans are opposed to targeted advertisements, even when their identity remains anonymous.[20] Despite claims that youths in particular "don't care" about privacy concerns involving geolocation, "most adult Americans (66%) do not want marketers to tailor advertisements to their interests."[21] In a 2009 survey conducted by Princeton Survey Research Associates International ("PRSA"), one thousand adult Internet users living in the United States were asked for their opinions on four topics: (1) tailored content and behavioral tracking; (2) rules of the marketplace in sharing information online and offline; (3) laws regarding information

---

[14] *Id*.

[15] Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It 5 (2009), *available at* https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

[16] Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 Fordham Intell. Prop. Media & Ent. L.J. 567, 570 (2012).

[17] Turow et al., *supra* note 15, at 9.

[18] *Id*.

[19] Dorothy M. Bollinger & Tristram R. Fall, III, *Current Developments in Privacy and Security-Impact of Technology*, 82 Pa. B.A. Q. 139, 140 (2011).

[20] Van Hal, *supra* note 13, at 728.

[21] Turow et al., *supra* note 15, at 3.

tracking and misuse of information; and (4) control over one's own personal information.[22] Based on the survey results, researchers were able to calculate statistics that reflect attitudes about targeted advertising.

Researchers concluded that Americans stand on the side of privacy advocates "in high percentages."[23] For example, "[e]ven when they are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% 'definitely' would not allow it, and 19% would 'probably' not allow it."[24] When people were informed about how providers gather data in order to tailor ads, between 73 and 86 percent "say they would not want such advertising." [25] Moreover, "69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them."[26]

The survey also revealed that the majority of Americans are misinformed about the current state of the law in this regard. For example, "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them."[27] Researchers noted that "[w]hen asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data."[28] This pattern suggests that Internet users have insufficient notice about the privacy policies involving data collected from geolocation services. "Most choose not to read them, for instance, and those that do find them unclear and excessively long."[29] Nevertheless, should users actually read the policies, they would likely be surprised to learn how few privacy safeguards are in effect.

When asked what type of punishment offenders should receive for violating informational privacy, the response was overwhelmingly in favor of strict guidelines. Specifically, "70% suggest that a company should be fined more than the maximum amount suggested ($2,500) if a company purchases or uses someone's information illegally."[30] Moreover, where a company "uses a person's information illegally. . . 18% choose that the company should be put out of business and 35% select that executives who

---

[22] *Id.* at 12.
[23] *Id.* at 3.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.* at 4.
[28] *Id.*
[29] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1032 (2012).
[30] Turow et al., *supra* note 15, at 4.

are responsible should face jail time."[31] Thus, it is clear that Americans largely reject targeted advertising and are concerned about the related privacy concerns.

In an attempt to determine why Americans are so opposed to targeted advertising, researchers considered two principal reasons. First, there may be "a general antagonism to being followed without knowing exactly how or with what effects."[32] Since people use the Internet for several different purposes (shopping, work, education, etc.), "Americans may not want their behavior on one site to somehow affect the interaction with subsequent sites."[33] Second, people may be afraid that "selective presentation of advertisements, discount offers, or news will put them at a monetary or social disadvantage: some people might get more useful or interesting tailored content than others depending on the conclusions marketers draw about them."[34] The concern with being labeled unfairly, and not being able to correct that profile, is a product of the lack of transparency between the companies gathering this information and consumers. Thus, "[i]f marketers want to continue to use various forms of behavioral targeting in their interactions with Americans, they must work with policymakers to open up the process so that individuals can learn exactly how their information is being collected and used, and then exercise control over their data."[35] Unfortunately, the current law does not operate in this fashion.

II. CURRENT LAW

The law governing use of geolocation services is largely undeveloped. Courts have not established a clear standard for handling claims alleging misuse of geolocational information without user consent or knowledge. Even the proposed Geolocational Privacy and Surveillance Act ("GPS Act") is overbroad and fails to effectively mitigate the problems raised by targeted advertising. Since courts have not had a chance to fully address this issue, this paper offers a proposed plan for dealing with geolocation claims.

There are few civil claims dealing with the wrongful use of geolocation. The case that is most on point is *In re iPhone/iPad Application Consumer Privacy Litigation*. In that case, plaintiffs sought class action certification "alleging, among other things, that the defendants, without the plaintiffs' knowledge, collected precise home and workplace locations and 'current whereabouts' of the plaintiffs by using certain features of iPhone and iPad operating systems and applications."[36] Plaintiffs filed claims under

---

[31] *Id.* at 24.
[32] *Id.* at 4.
[33] *Id.*
[34] *Id.* at 4.
[35] *Id.* at 5.
[36] Theodore F. Claypoole & Richard C. Balough, *Developments in the Law*

the Stored Communications Act, the Wiretap Act, the Computer Fraud and Abuse Act, and the California Constitution, all of which were dismissed by the court.[37] In fact, the court "allowed only two counts against Apple to proceed, but those counts concern misrepresentations rather than a right of privacy regarding geolocation."[38] To date, courts "have not considered geolocation to be highly intrusive," and no court other than the Northern District of California has considered whether a right of privacy exists with regard to geolocation.[39]

The other two cases that bear most on the issue of geolocation are still pending in court. The first, *Cousineau v. Microsoft Corp.*, alleges that "even after a user clicked to deny Microsoft access to her geolocation, Microsoft continued to collect the information."[40] Plaintiffs assert that "Microsoft surreptitiously forced even unwilling users into its non-stop geo-tracking program in the interest of developing its digital marketing grid."[41] The other, *Goodman v. HTC America, Inc.*, alleges that "a mobile phone manufacturer and application developer installed a local weather application ostensibly to provide convenient weather reports, but they subsequently used the application to transmit the plaintiffs' locations for other purposes, including for 'fine' geographic location data, which identifies the latitude and longitude of a particular device's location within several feet at a given date and time."[42] Pending before the court is defendant's motion to dismiss for failure to allege any injury.[43] It is feared that these cases will be dismissed because the alleged damages are too speculative.

Another source of law involving geolocation services is pending approval in Congress. The proposed GPS Act would "prohibit any 'Person' from intentionally intercepting or disclosing location data and the use of location information by any person knowing or having reason to know that the information was obtained through the interception of such information in violation of the Act."[44] The Act would require probable cause and a warrant for a governmental entity to obtain geolocational information.[45] For private companies, businesses would be prevented from sharing

---

Concerning Geolocational Privacy, 68 Bus. Law. 197, 202 (2012).

[37] *See In re* iPhone/iPad Application Consumer Privacy Litigation, 844 F.Supp.2d 1040 (N.D. Cal. 2012).

[38] Claypoole, *supra* note 36, at 202.

[39] 4 Ian Ballon, E-Commerce and Internet Law: Treatise with Forms § 58.06[7] (2d ed. 2012-2013 update).

[40] Claypoole, *supra* note 36, at 201.

[41] Cousineau v. Microsoft Corp., No. 11-cv-01438-JCC (W.D. Wash. filed Oct. 17, 2011).

[42] Claypoole, *supra* note 36, at 202.

[43] *See* Goodman v. HTC America, Inc., No. 11-cv-01793-MJP (W.D. Wash. filed Jun. 26, 2012).

[44] Claypoole, *supra* note 36, at 203.

[45] *Id.*

geolocational information without explicit consent of the individual.[46] The remedy for violations under the Act are "actual and punitive damages, or statutory damages of $100 per day or $10,000 total."[47]

Critics of the proposed legislation argue that it is overbroad and does not establish requirements for the consent necessary to disclose information. Some have argued that "the proposed statute applies a broad probable cause requirement to virtually any request from a service that collects location data."[48] The proposed statute governs all "geolocational information," defined as "any information . . . concerning the location of a wireless communication device . . . that could be used to determine or infer information regarding the location of the person."[49] But the problem with trying to apply one standard to all types of geolocation is that it fails to consider the intricacies and nuances of these emerging technologies. The same standard governs "the entire spectrum of location data, from the suspect's location when he made a single phone call to four months' worth of driving patterns."[50]

The proposed statute also falls short in defining the consent necessary for a private company to track a consumer's movements and then disseminate that information. Indeed, "the GPS Act does not prescribe language that must be included in a request for a customer's consent to disclose information."[51] It simply requires that consent be "lawful."[52] This is awfully vague, perhaps intentionally. But having a vague standard with regard to consent opens up the potential for abuse. For example:

> When consumers choose to give consent to access their information, the decision often is only partially informed. This is especially true if consent to sharing is required as a prerequisite of receiving service. In a consent-based data sharing system, moreover, the service provider "has an incentive to exaggerate the scope" of the information that it requests in order to maximize the breadth of the consent that it receives.[53]

Thus, to mitigate these risks, Congress should prescribe specific language required for all consent requests and the "amount of time for which a

---

[46] Geolocational Privacy and Surveillance Act, S. 639, 113th Cong. (2013).

[47] *Id.* §2605(b)(2), (c)(1)-(2).

[48] Matthew Radler, *Privacy Is the Problem: United States v. Maynard and A Case for A New Regulatory Model for Police Surveillance*, 80 Geo. Wash. L. Rev. 1209, 1240 (2012).

[49] Geolocation Privacy and Surveillance Act, S. 1212, 112th Cong. §2601(4) (2011).

[50] Radler, *supra* note 48, at 1240.

[51] Sonia K. McNeil, *Privacy and the Modern Grid*, 25 Harv. J.L. & Tech. 199, 223 (2011).

[52] *Id.*

[53] *Id.*

consumer's consent is valid" should be limited.[54] Ultimately, as I explain in the next part, it is clear that the GPS Act is unnecessary and common law could solve the privacy concerns involving geolocation.

III. PROPOSED CHANGES

To better address the growing privacy concerns related to use of geolocational information, two changes should be enacted: (1) create legislatively-enacted consent and disclosure requirements; and (2) apply the tort of intrusion on seclusion to claims involving geolocational privacy. Unlike the GPS Act, these changes would narrow the scope of protection and thus create an effective system of handling claims involving geolocational privacy.

Arguably the biggest privacy concern related to geolocation is that users give consent presumably without fully understanding the consequences. To reduce that concern, lawmakers should look to outside laws governing geolocation to find the system that best fits the United States. For example, the Working Party in the European Union issued an opinion on geolocation in 2011, which identifies privacy concerns and how to best address those issues. Their approach features "comprehensive national laws, prohibitions against collection of data without a consumer's consent and requiring companies that process data to register their activities with government authorities."[55] More specifically, the Working Party has opined that "[c]onsent must be specific, informed and freely given, and can be withdrawn at any time."[56] In addition, since opt-out mechanisms are usually ineffective, "the Working Party is in favor of requiring users to renew their consent at least once a year."[57]

With the goal of more informed consent in mind, the United States should adopt similar principles, but should also formulate specific language that must be included in consent requests. There should be several requirements in giving consent: (1) in the terms of service, cell phone or Internet providers must obtain affirmative consent of the user before the company can use geolocational information for any purpose, including targeted advertising; (2) users must be permitted to revoke consent at any time by reviewing the terms of service and opting out of geolocation services, and that if consent is revoked, the company will not gather, use, or disseminate geolocational information at any time but instead will delete

---

[54] *Id.* at 224.

[55] Daniel L. Pieringer, *There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications*, U. Ill. J.L. Tech. & Pol'y, 559, 574 (2012).

[56] Hunton & Williams LLP, *Article 29 Working Party Opines on Geolocation Services*, Cyberspace Lawyer, June 2011, at 19, 20.

[57] *Id.*

such data, no more than thirty days after the user's revocation of consent; (3) providers must make clear what they intend to use geolocation services for, and must state that "should a user give consent for use of geolocational information, he/she authorizes the company to gather information based on a user's prior purchases, web site clicks, physical store visits, and other locational-based interests gathered from both online and offline activity"; and (4) users shall be required to renew their consent every year that consent is given. These principles would accomplish both the goals of heightened notice and consent, leading to more informed decisions about whether a user wants the benefits of geolocation services or prefers to shield himself or herself from inherent privacy concerns.

Second, the tort of intrusion on seclusion should apply to adjudication of claims involving geolocational information. It appears that this law "offers the best theory to target legitimate privacy harms in the information age."[58] Basically, this tort imposes liability on any person or entity "who intentionally intrudes . . . upon the . . . seclusion of another . . . if the intrusion would be highly offensive to a reasonable man."[59] The premise behind the tort is to protect the "right to respite from observation and judgment so that, when we do participate socially, we can be more engaged and ethical participants."[60] The relevant inquiry is not whether the content of the information collected is an intrusion, but rather whether the observation or monitoring itself is offensive.[61] Thus, a "voyeur who peers through the windows and observes a mundane family scene has intruded upon the family's seclusion even though he has not learned any secrets."[62]

Although the tort was originally designed for conduct in real space, its principles apply equally as well to information in the electronic age. For example, suppose a company began monitoring a person's movements throughout a grocery store and recorded every product that person considered buying, but did not. While this scenario is outlandish in the real world, it happens daily in the online context simply by using geolocational information. Since this behavior would clearly be offensive to a reasonable person in the real world, it too should apply to practices in e-commerce.[63]

This approach to handling privacy concerns would not eliminate targeted advertising altogether. Instead, "[i]nformation flow should be deterred through liability rules when, and only when, the foreseeable privacy harms outweigh the benefits of free-flowing facts."[64] Thus, those

---

[58] Jane Yakowitz Bambauer, *The New Intrusion*, 88 Notre Dame L. Rev. 205 (2012).
[59] Restatement (Second) of Torts §652B (1977).
[60] Yakowitz, *supra* note 58, at 206.
[61] *Id.*
[62] *Id.* at 231.
[63] *See id.* at 206.
[64] *Id.* at 227.

who consent to use of geolocational information would have no claim under intrusion on seclusion. Moreover, it would avoid conflict with the First Amendment because "the intrusion tort regulates behavior," not speech or the free flow of information.[65] Courts have already determined that federal statutes like the Wiretap Act, Stored Communications Act, and Computer Fraud and Abuse Act are not unconstitutional under the First Amendment.[66] Adjudicating matters under the tort of intrusion on seclusion would similarly pass constitutional tests.

Proponents of using this tort in the context of geolocational information point to the fact that it "reinforces norms by tracking social consensus, which means that most people will recognize what is and is not seclusion, even in new contexts."[67] This flexibility to adapt to changing technologies is ideal in the realm of geolocation, as companies are rapidly developing new ways to reach consumers and generate advertising profiles based on interests, prior purchases, and store visits. This is particularly favorable as compared to the GPS Act, which does not have the "highly offensive" limitation.

The injury that plaintiffs may assert in a claim for intrusion on seclusion is directly related to the requirement of consent. If a data collecting company gathers information without the prior consent of the consumer, or a consumer has given but since revoked their consent, courts would likely find that this observation is unreasonable. This would effectively create a bright-line rule that monitoring activity without informed consent is illegal per se. Although some location collection is allowable under the tort, only those plaintiffs who can demonstrate harm would be able to make a *prima facie* claim. Finally, since there is strong public support in favor of banning the collection of location-based data without consent, the interests of society would be advanced by adjudicating matters under the tort of intrusion on seclusion.

* * *

In conclusion, there is a real need for heightened protections in the context of geolocation services and the subsequent transmission of that personal information for targeted advertising. Studies have indicated that there is strong public opinion against the use of geolocation for targeted advertising, even when anonymity is preserved. To more accurately reflect the clear societal views towards geolocation, notice and consent must be a greater focus. Creating stricter requirements for consent requests, providing

---

[65] *Id.* at 231-32.
[66] *Id.* at 232.
[67] *Id.* at 235.

for clearer notice regarding the use of geolocational information, and applying the tort of intrusion to geolocation observation would best accomplish these goals. Under this new system, fears about the collection, use, or dissemination of geolocational information would be quelled.