Geolocational Technologies and Privacy

By Richard Balough and Ted Claypoole

Co-Chairs of the Cyberspace mCommerce Subcommittee

Is there any expectation of location privacy today? As you strolled down the street today, how many times was your image captured? Are you concerned that your cell phone tracks your every move? Is your car equipped with an automatic device to pay tolls as you drive down the highway, leaving an easily followed trail? Are you concerned that the government can track your every move? Does the Constitutional right of free assembly include the right to meet and talk in private?

The latest iPhone software combines your location with your questions to provide a voice response. You can be reminded to pick up a loaf of bread when you leave your office, which is triggered when you actually leave the office. In other words, it knows the exact location of your office and the time you leave it. On foursquare, friends can share their location with each other and check in at certain locations, where you can earn points or merely meet up with other users. Facebook and LinkedIn users frequently notify their friends of their location or when they leave on trips.

As communications and transactions move to the mobile environment, legislators, regulators, and the courts are beginning to struggle with questions concerning geolocation. As a society, we have evolved from colonial times when a person could simply walk away from the from or step outside of town for a private moment. With geolocation tracking, someone knows where we are at all times.

Does anyone care that they can be followed 24/7 by technology? Should people be concerned that this information is being accumulated and is readily available?

Over a hundred years ago, Samuel D. Warren and Louis D. Brandeis observed:

> The intensity and complexity of life, attendant upon advancing civilizations, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

4 Harv. L. Rev. 193, 196. At the time, the authors were concerned about "instantaneous photographs" and mechanical devices that threatened "to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" *Id*. at 195. These concerns caused them to conclude that there should be a right to privacy for individuals under certain circumstances.

There is no specific provision in the U.S. Constitution granting a "right of privacy." However, the Supreme Court has crafted a right of privacy, at least as far as governmental intrusion, through the Fourth Amendment search and seizure provisions and the Fourteenth Amendment due process provisions. In *Griswold v. Connecticut,* 381 U.S. 479, 485 (1965), the Supreme Court stated:

> The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the *use* of contraceptives rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a "governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms." *NAACP* v. *Alabama*, 377 U.S. 288, 307. Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.
>
> We deal with a right of privacy older than the Bill of Rights -- older than our political parties, older than our school system.

This right of privacy is the basis for many other court decisions.

In 1989 the United States Supreme Court similarly found that the disclosure of a private citizen's "rap sheet" to third parties constituted an unwarranted invasion of privacy, holding:

> . . . as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted."

United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 780 (1989). In that case, a journalist had requested under the Freedom of Information Act (FOIA), 5 USCS 552, that the Justice Department and Federal Bureau of Investigation disclose criminal records of four brothers whose family's company allegedly had obtained defense contracts as a result of an improper arrangement with a corrupt Congressman. The court looked to the exception from disclosure under FOIA of "personnel and medical files and similar files the disclosure of which would constitute an unwarranted invasion of privacy." *Id.* at 758. The court found that a rap sheet is a "similar file" because "rap-sheet information 'is personal to the individual named therein.'" *Id.*

The court further found that the balancing test required it "to balance the privacy interest in maintaining, as the Government puts it, the 'practical obscurity' of the rap sheets against the public interest in their release." *Id.* at 762. The interest for the family was characterized by the court as "avoiding disclosure of personal matters." The court defined "both the common law and the literal understandings of privacy [to] encompass the individual's control of information concerning his or her person." Therefore, "[p]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.* at 764. "In sum, the fact that 'an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information.'" *Id.* at 770.

With the Internet, public records not only are not in "practical obscurity" but rather are only a Google search away. Yet, the language in the *Reporters Committee* case is at the forefront of the

question of geolocational privacy before the United States Supreme Court this term. At issue in *United States v. Jones* is the question of whether tracking an individual's car with a GPS device for 28 days violates the Fourth Amendment as an "unreasonable search." Law enforcement officers had placed a GPS tracking unit on Jones' vehicle without a warrant. Jones was convicted in the trial court of conspiracy to distribute cocaine.

The appellate court threw out the conviction, finding that use of the GPS tracking device for such a lengthy period of time required a warrant. *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).[1] The court found that, while a person has no expectation of privacy while on a public thoroughfare, the use of the GPS device was not used to track movements from one place to another "but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place." *Id.* at 558.

> [W]e hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.

Id. at 560. The court noted that *Reporters Committee* upheld the privacy exception to FOIA even though the individual convictions were public because the sum of the parts can exceed each part individually. Because the rap sheets were in different locations, there was a "practical obscurity" for the facts, which prevented an expectation that the information would be gathered in one location. Similarly, the *Maynard* court in found that a "reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each

---

[1] The *United States v. Jones* case currently before the U.S. Supreme Court was captioned in the appellate court as *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

place he stops and how long he states there. Rather, he expects each of these movements to remain 'disconnected and anonymous.'" *Id*. at 563. Reflecting the reasoning in *Reporters Committee*, the *Maynard* court stated that the:

> whole reveals far more than the individual movements its comprises. . . Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. . . Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month . . . . A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Id. 561-562.

The holding in Maynard is directly contrary to *United States v. Cuevas-Perez*, a Seventh Circuit case. 640 F.3d 272 (7th Cir. 2011). Cuevas-Perez's car was tracked for 60 hours during a road trip through New Mexico, Texas, Oklahoma, Missouri, and finally Illinois, where the GPS battery gave out, requiring the Immigration and Customs Enforcement agents to ask that the Illinois police follow his car and pull him over for any type of violation, which they did. The court said *Maynard* "is wrongly decided." *Id*. at 276. However, in a dissent, Judge Wood found that a prolonged GPS surveillance

> intrudes upon an individual's reasonable expectation of privacy by revealing information about her daily trajectory and pattern that would, as a practical matter, remain private without the aid of technology. . . To conclude that open-ended, real-time GPS surveillance is not a 'search' invites an unprecedented level of government intrusion into every person's private life. The government could, without any metric of suspicion, monitor the whereabouts of any person without constitutional constraint. Under the majority's view, such surveillance is tolerable. Thus, not only is the indefinite GPS surveillance of a single person permissible; the government could also keep tabs on entire communities, perhaps with the hope of identifying hints of criminal conduct.

Id. at 294.

Whether there is any expectation of privacy also is being raised where the government seeks records that identify the base station towers and sectors for cell phones. With this

information, the government can determine a person's exact location when placing calls, emailing, or texting. The question is whether the information falls under the Fourth Amendment. Under the Stored Communications Act, 18 U.S.C. §2703, the government can require disclosure of records pertaining to a subscriber or customer only when the government obtains a court order for such disclosure. The order "shall issue only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe" that the communication are relevant to an ongoing criminal investigation. 18 U.S.C. §2703(d). This showing is lower than probable cause required for a warrant.

In the Matter of An Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, a district court in New York denied the government's request for cell tower information. The court noted that the use of "cell-site location records present even greater constitutional concerns than the tracking at issue in Maynard." The court found that cell-site location records enable the tracking of the vast majority of American.

> Thus, the collection of cell-site location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.

2011 U.S. Dist. Lexis 93494*17-18.

The court rejected the argument that a cell-phone user voluntarily discloses his location by turning on his phone and making and receiving calls and text messages. "Applying the third-party-disclosure doctrine to cumulative cell-site-location records would permit governmental intrusion into information which is objective recognized as highly private." Id. at *37.

The issue of the use of cell phones to determine a person's location also has arisen outside the criminal area. In *Cousineau v. Microsoft Corp.,* W.D. Washington No. 2:11CV0438, the plaintiff is seeking class action status in a complaint against Microsoft. The case involves whether the Microsoft Windows Phone 7 application surreptitiously forced users into its non-stop geo-tracing program. The plaintiff alleges that even when a user turned off the tracking feature, the information still was sent to Microsoft. In response, Microsoft said there was a software error in the code. Microsoft has filed a motion to dismiss the case.

In *Clements-Jeffery v. City of Springfield*, 2011 U.S. Dist. Lexis 93593, the issue concerned a laptop computer recovery program. When a laptop is reported stolen, the program is activated. When the laptop is connected to the Internet, it secretly sends back the IP address of the user along with screenshots. Clements-Jeffery bought a laptop that had been stolen. She used the laptop to communicate with her boyfriend, sending explicit webcam pictures. The webcam pictures were viewed by the Springfield police, who made repeated comments to her about the webcam images of herself. The charges against her were dismissed. She sued for violations of the Electronic Communications Privacy Act, the Stores Communications Act, and common law invasion of privacy. The City moved for summary judgment. The court rejected the request for summary judgment on the right to privacy count because there was a question of fact as to whether Clements-Jeffery knew or should have known that the laptop was stolen. If she did not know, the court reasoned that she had an expectation of privacy. The case was settled.

Another method of addressing the unanticipated loss of privacy due to intrusive use of mobile device data is to sue the manufacturers for breaching promises or for violation of the consumer protection laws. One of the first cases to claim that intrusive and unprotected software

is a consumer defect under the consumer protection laws is the recent filing of *Goodman v. HTC America* [referred to as the *AccuWeather* Case][2], filed in the United States District Court, Western District of Washington at Seattle. The Plaintiffs in this matter alleged that a mobile phone manufacturer and application developer installed the AccuWeather application on their phones ostensibly to provide convenient weather reports, but subsequently used the application to transmit plaintiffs' locations for other purposes (including "fine" geographic location data, which identifies the latitude and longitude of a particular device's location within several feet at a given data and time). Plaintiffs also claimed that defendants failed to meet accepted baseline information security standards (by transmitting the information in an unencrypted manner), and acknowledged a product defect but failed to alert purchasers, rectify the defect, investigate data usage and/or onward transfer of detailed geographic location data, or remediate the third-party retention of the data.

This case should reverberate far beyond Puget Sound because the plaintiffs claim class representation and the complaint alleges violations of Minnesota's Prevention of Consumer Fraud Act (the Defendants engaged in consumer fraud by failing to disclose the defects in the Smartphone product), Minnesota's Unlawful Trade Practices Act (the Defendants mislead consumers as to the quality of the product), California's Consumer Legal Remedies Act (the Defendants represented that the smart phones with the integrated app were defect-free), and California's Business and Professional Code (the Plaintiffs had a reasonable expectation that the devices would be defect-free and designed and functioning according to reasonable security standards).

---

[2] Case number 2:2011cv01793, filed October 23, 2011.

The AccuWeather application apparently cannot be uninstalled or easily disabled, allowing the Plaintiffs to claim that Defendants had intentionally planted a Trojan horse application on their phones masked as a weather guide. Ultimately this case may serve as the basis for consumers to classify overly intrusive software and hardware as violating Federal and various state consumer protections laws, and to forum shop for the laws most likely to support their favored conclusions.

Apple Computer, as one of the dominant providers of mobile technology has been questioned this year on what information Apple is capturing from its customers and how it is using that information. Apple has been questioned by Congress and sued, and then Apple reacted to concerns about use of the UDID for their iphones and ipods. Apple has been forced to revise its data capture methods in response to regulatory scrutiny, although the company has not been entirely open about its practices.

In late April of 2011, Researches published their findings that Apple was tracking users and tying them to unique telephone IDS (UDID). The researchers stated that Apple is secretly compiling longitude and latitude for users every day and sending this data back to Apple during synch actions online, sometimes logging precise geolocation 100 times a day. These files were allegedly sent and stored in unencrypted format. The research paper revealed that Apple was routinely storing tracking data on Apple iPhones and iPads in a secret file "consolidated.db.".

Congress, specifically Representative Markey and Senator Franken, sent letters requesting an explanation from Apple about its use of location data sharing on Apple mobile

products.[3] Without being too specific about what it was doing with the data or who else was seeing the data, Apple testified that it needs to use this data.[4]

Apple received a class action complaint related to the same set of information. In *Vikram Ajjampur v. Apple, Inc.*[5] filed in the United States District Court Middle District Of Florida, Tampa Division, the Plaintiffs allege that Apple iPhones and 3G iPads are secretly recording and storing details of all their owners' movements, and

> "According to security experts Alasdair Allan and Pete Warden, the location data is hidden from users but unencrypted, making it easy for Apple or third parties to later access. Apple Inc.'s iPhone Tracks Users' Movements, April 20, 2011. Collection of this information is "clearly intentional." Users of Apple products have to no way to prevent Apple from collecting this information because even if users disable the iPhone and iPad GPS components, Apple's tracking system remains fully functional."

This class action lawsuit uses the researchers data and charges Apple with violations of the law for taking this information and for not protecting it at rest or in transit. The suit alleges that Apple covertly collects and stores users' location data from the plaintiffs' mobile devices (iPhones and iPads) in violation of the Computer Fraud and Abuse Act and Florida's Computer Crimes Act, and without notice or consent (just as if they were personally tracked by a tracking device for which a court-ordered warrant would ordinarily be required); in many cases this information was highly personal (e.g. information to which employers and spouses were not privy). The Plaintiff's cited and alleged violation of the consumer protection laws of all fifty states.

---

[3] http://abcnews.go.com/Technology/apple-pushed-congress-answers-iphone-tracking/story?id=13426917#.TuzBxjWvKSo

[4] http://consumerist.com/2011/04/apple-tells-congress-it-must-have-controversial-user-location-data.html See Also: http://news.cnet.com/8301-27076_3-20061479-248.html

[5] Case 8:11-cv-00895-RAL-TBM, filed April 22, 2011.

Allegations include that the data is unencrypted (on both the mobile devices and on users' computers that sync with those devices) and publicly accessible, which puts plaintiffs at serious risk of privacy violations (including stalking); defendants' terms of service do not disclose its tracking of users, and its privacy policy is unfair, deceptive and misleading (e.g. ordinary consumers would not understand defendant's privacy policy to include the location tracking and syncing, and were deceived into believing their movements would not be stored for future use in a defendant-designed database). Plaintiffs seek declaratory relief and treble or punitive damages against Apple.

In response to public concern over the collection of location data, Apple released a software update for mobile devices, available through iTunes. The update will limit the storage of location data to one week, stop the transfer of location data when the device is synched, and erase all location data from a device if a user turns off Location Services. Location data stored on the device will also now be encrypted.

Nor has dominant search company Google escaped from mobile privacy scrutiny. While not as directly related to mobile devices as the Apple cases, Google has clearly requested that Congress clarify mobile privacy rules to avoid stifling innovation in the space.[6] Google collects similar data to Apple in mobile space, but is more dangerous to privacy because of all the other information that can be aggregated with it, including Google's admitted capture of private email content.

---

[6] See, http://www.infosyncworld.com/reviews/cell-phones/google-urges-congress-to-act-on-privacy-immediately/12014.html .

For example, in the case of *In Re Google Street View Electronic Communications Litigation*[7] the Court determined that Google is not exempt from liability under the Wiretap Act for using wireless sniffer technology to collect, decode and analyze payload data broadcast through Wi-Fi connections; although there is an exemption for electronic communications made through a system configured to be readily accessible to the public, communications sent via Wi-Fi technology are not designed or intended to be public, and merely pleading that a network is unencrypted does not render that network "readily accessible to the general public" (the fact that a network is unencrypted does not remove the intentional interception of electronic communications from that network from liability under the Wiretap Act). The claim under California's Unfair and Deceptive Business Practices law was dismissed as the plaintiff's failed to plead in injury sufficient for standing (interception of data packets that a plaintiff has sent over a wireless network are not lost property for purposes of determining standing).

EPIC also had a case against Google regarding the capture of information while setting up Google Streetview, and EPIC settled the case this year.[8] EPIC and the Federal Trade Commission agreed to settle an open government lawsuit concerning the FTC's decision to close the investigation of Google Street View. EPIC sought documents from the Commission after Members of Congress had urged the agency to pursue an aggressive investigation and many privacy agencies around the world found that Google violated national privacy laws. The agency turned over to EPIC agency records which suggested that the agency believed it lacked enforcement authority. However, the closing letter in the case also indicated that the Commission

---

[7] 2011 U.S. Dist. LEXIS 71572, N. Dist of California, June 29, 2011.

[8] EPIC v. FTC, No. 11-cv-00881 (D.C. Dist. Ct 2011).

never undertook an independent investigation to determine whether other violations of law may have occurred.

EPIC has a number of privacy gripes against the current Google business models. Supporting its FTC case in the Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief *In the Matter of Google, Inc*., EPIC recommends that the FTC should include the following: require fair information practices for all of Google's products and services (this would build on the principles of transparency, user control, and security and would draw on the OECD guidelines and the Privacy Act of 1974); keep non-Gmail users' emails fully private (non Gmail users who are emailing a Gmail user have not consented to their communications being analyzed or to the creation of a profile about them and their emails are being analyzed to provide targeted content to Gmail recipients); end the collection of data transmitted by residential wireless routers (Google Street View collects information that is tied to location information, i.e. unique device IDs for Wi-Fi hotspots and user-assigned network names); make results of Google's privacy assessments available to the public; apply the provisions of the consent agreement to all other Internet companies (thereby addressing anti-trust concerns); build a do not track mechanism into the Chrome web browser (rather than only allowing for opt-out of cookies); and cease tracking mobile phone users' locations or web-browsing habits without opt-in consent (Android phones collect location data and users may opt-out of this service by unchecking a box that is checked by default).

The FTC has recently released a statement on protecting mobile privacy in the age of geotracked smartphones. See, Prepared Statement of the FTC on Protecting Mobile Privacy: Your Smart phones, Tablets, Cell Phones and Your Privacy- United States Senate, Committee on the Judiciary (May 10, 2011); Also see, FTC prepared statement on Consumer Privacy and

Protection in the Mobile Marketplace before the Senate Committee on Commerce Science and Transportation (May 19, 2011).[9]

In the statements, the FTC applies section 5 of the FTC rules to the mobile arena. The Commissioners describe and note several cases for deceptive privacy notices in the mobile space and for sending unsolicited text messages, including cases regarding insufficient safeguarding of customer mobile phone information and the case of a company self-posting strong reviews of its own games and the FTC charged it with deceptively advertising for mobile gaming applications by pretending that the reviews came from disinterested users.

The FTC noted the "virtually ubiquitous data collection by smart phones and their apps (such as age, gender, precise location and unique phone identifiers), and testified that mobile devices can facilitate data collection and allow companies to collect users' data over time to reveal habits and patterns. The Commission believes that mobile phone and app companies should provide stream-lined privacy choices easily readable and accessible on a mobile phone's screen, and not collect or retain more data than needed to provide a requested service or transaction. The FTC staff report noted the problems with effectively presenting options on such small mobile devices.

The FTC staff report on this topic questions where Do Not Track rules should be applied to mobile providers of equipment and applications. They suggest that the consumer's browser would remember the Do Not Track choice and request that visited web sites not track the consumer. The Commission notes special concern for the mobile privacy of children and teens, including stringent protection of the Children's Online Privacy Protection Rule. For example,

---

[9] Information Law Group Summary of Testimonies accessible: http://www.infolawgroup.com/2011/05/articles/data-privacy-law-or-regulation/senate-subcommittee-holds-hearing-on-mobile-privacy/ .

the Commission announced a $3 Million settlement against Playdom, Inc. for violating COPPA.[10]

[10] Statements Accessible at: http://www.ftc.gov/os/testimony/110510mobileprivacysenate.pdf (5/10/2011); 5/19/11 Statement: http://commerce.senate.gov/public/?a=Files.Serve&File_id=4d7843ad-9b6c-4b09-a1d0-de9150b78ca3 .