BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Privacy Considerations Limit Geolocation Technologies

By Ted Claypoole and Richard C. Balough

American courts are beginning to place limits on the previously unrestricted use of location-tracking technology. In both law enforcement cases and consumer litigation, litigants and judges are drawing lines that define the degree to which Americans may be tracked, followed, and surveilled using cost-effective location-reporting devices.

This trend toward greater restrictions is important as the cost of constant location reporting plummets so that parents, employers, jealous lovers, and law enforcement officials can simply follow every step taken and mile driven by a targeted individual, and as each of us brings the implements of pervasive location tracking––especially new cars and smartphones––with us wherever we travel. In addition, better awareness of tracking technology has led to new applications like Foursquare, Facebook Maps, and Google Latitudes, which broadcast people's present spot on the globe. Law enforcement has also become more sophisticated in using both stationary cameras and location-monitoring systems like EZPASS, as well as the many ways that cell phones can pinpoint a person's location.

This article examines the United States' judicially recognized privacy rights, including those dealt with in the recent *Jones v. United States* case addressing location privacy in January 2012 by the U.S. Supreme Court, and discusses recent trends in legal claims demanding better mobile privacy of personal location. The narrowly decided *Jones* case is likely to be an early shot in the war for geolocation privacy and is far from the final battle. The various *Jones* opinions and recently filed cases support this conclusion. Business lawyers will best serve their clients by carefully watching this rapidly changing technology field and the legal restrictions placed on the use of geolocation technology.

Location Tracking Devices are Part of Today's Society

Many people are concerned about the insidious creep of location-tracking technology into our lives. For example, the latest iPhone software includes your location to answer your questions with a voice response. Your reminder to stop for a loaf of bread when you leave your office 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 locations with each other and check in at certain sites, 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 a society, we have evolved from colonial times when a person could simply walk away in the dark or step outside of town for a completely private moment. At that time, entire armies disappeared for days, and a ship leaving port may not have been heard from for months or years, if ever. With today's geolocation tracking, someone knows where we are at all times. Over a hundred years ago, Justices 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 (1890).

At the time, the authors worried 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.'" 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" in those words. However, the Supreme Court has crafted a right to protect private matters from certain 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. . . . 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, including cases relating to the privacy of personal conversations. In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court held that wiretapping a telephone booth violated the reasonable expectation of privacy that a person had in his conversation over that phone line and that, because the Fourth Amendment protects people, and not places, a government "trespass" on private space was not necessary to prove the government violated a person's Fourth Amendment rights. The court held that Fourth Amendment protections do not rely on the presence of a physical intrusion by the government.

Technology Has Made Practical Obscurity Obsolete

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 that an invasion of privacy is unwarranted if the "practical obscurity" of certain information outweighs the public interest in publicizing the information. *United States Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, 780 (1989). With the Internet, public records not only are not in practical obscurity, but rather are only a Google search away.

The U.S. Supreme Court recently addressed the intrusion on practical obscurity of an individual's location in *Jones v. United States*, ___ U.S. ___ (2012), analyzing whether a drug-dealing conviction could hinge on 28 days of location monitoring from a tracking device placed on a suspect's car without a warrant, when the device reported the suspect's location every 10 seconds for the entire period. While the police had originally obtained a warrant to track the suspect's car, that warrant had expired by the time the tracking device was placed.

The appellate court had thrown 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). The lower court found that, while a person has no expectation of privacy while on a public thoroughfare, 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 place he stops and how long he stays there; rather, he expects each of these movements to remain disconnected and anonymous." Reflecting the reasoning in *Reporters Committee*, the *Maynard* court stated that "[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."

The holding in *Maynard* was directly contrary to other geolocation tracking decisions, including *United States v. Cuevas-Perez*, 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 divided *Cuevas-Perez* court said *Maynard* "is wrongly decided."

Warrant Required for Tracking Device on Car

This conflict was tangentially addressed by the Supreme Court in *Jones*, which unanimously agreed that surreptitiously placing a tracking device on a suspect's car and electronically tracking the car everywhere for a number of days could not be conducted without a judicial warrant. The five-member Court majority held that deciding this case did not demand a review of whether the police's actions intruded on the suspect's reasonable expectation of privacy as described in the *Katz* case above. Instead, it held that the police trespassed on the suspect's car when placing the tracking device there. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures," and the suspect's car was an "effect" protected against unwarranted trespass by the government. This majority opinion stated that the *Katz* "reasonable expectation of privacy" test for Fourth Amendment cases added to the prior case law based on trespass to property, and since the placement of tracking devices was a "search," then it must be a reasonable search under the law.

However, another important aspect of the *Jones* case can be found in the various concurring opinions to the majority's holding, where four members of the court accuse the majority of shirking its responsibility to address the true "vexing problems" of the *Jones* case, including whether the simple act of electronically monitoring a suspect for 28 days without a warrant is allowed under the Fourth Amendment. The primary concurrence accuses the majority of relying on "18th Century Tort Law" to avoid deciding the important issues of personal privacy in this age of technological surveillance. It is clear from a reading of *Jones* that the entire Supreme Court believes it is likely that the *Jones* majority opinion is not the final word on the government's obligations when using location-tracking equipment. Even Justice Scalia, in his majority opinion, states, "We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."

Justice Alito, writing for a four-judge minority of the Court, felt that the *Jones*

case should be decided against the government because the tracked suspect had a reasonable expectation that his movements would not be electronically monitored every 10 seconds for four straight weeks. Justice Sotomayor, who joined the majority opinion, also wrote a concurrence in which she credited Justice Alito's arguments, but found that the facts of the *Jones* case could be decided more effectively by addressing the government's physical trespass on the suspect's vehicle. So we may easily believe that there is at least a majority of Justices who agree with Justice Alito's broader argument, although Justice Sotomayor did not choose to apply this argument to the specific fact pattern before the Court in *Jones*.

Justice Alito notes that purely electronic surveillance, such as activating a stolen-car tracking system or monitoring phone movement through cell tower triangulation would have created the same effect on the suspect without a trespass that the majority opinion relied upon for its decision. Justice Alito and his concurring coalition find both tracking methods––physical and electronic––equally objectionable without a warrant. While Justice Alito invited legislative action to clarify law enforcement's obligations in regard to long-term electronic location tracking, he found that, with or without a physical trespass, four weeks of warrantless surveillance was clearly out of bounds, and the government's actions violated the suspect's reasonable expectation of privacy.

Using Triangulation Raises Constitutional Concerns

In other geolocation tracking cases, courts have questioned the extent of a person's privacy expectation where the government seeks records that identify and triangulate the base station towers for cell phones. With this information, the government can determine a person's exact location when placing calls, e-mailing, or texting. But is such electronic tracking a search under the Fourth Amendment? Pursuant to the Stored Communications Act, 18 U.S.C. §2703, the government may demand disclosure of records pertaining to a subscriber only with a court order, which "shall issue only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe" that the communication is relevant to an ongoing criminal investigation. 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 Americans: "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." 2011 U.S. Dist. Lexis 93494 *17–18. The court rejected the argument that a cell-phone user voluntarily discloses his or her location by turning on a phone and making and receiving calls and text messages.

Embedded Software Tracking: Private Cause of Action

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

Another approach 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 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* (the *AccuWeather* case), Case Number 2:2011cv01793, filed October 23, 2011, in the United States District Court, Western District of Washington. The plaintiffs 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 date, 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. The plaintiffs claim class representation and the complaint alleges violations of specific consumer laws in several states.

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 also received a class action complaint related to its collection of customer location information on iPhones. In *Vikram Ajjampur v. Apple, Inc.*, Case 8:11-cv-00895-RAL-TBM, filed April 22, 2011, in the United States District Court, Middle District of Florida, the plaintiffs allege that Apple iPhones and 3G iPads are secretly recording and storing details of all their owners' movements, and

> the location data is hidden from users but unencrypted, making it easy for Apple or third parties to later access. . . . 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 lawsuit charges Apple with violations of the law for taking this information and for not protecting it at rest or in transit. The plaintiffs cited an alleged violation of the consumer protection laws of all 50 states, based on allegations that the data is unencrypted (on both the mobile devices and on users' computers which synch with those devices) and publicly accessible, which puts plaintiffs at serious risk of privacy violations (including stalking), that Apple's terms of service do not disclose tracking of users, and that ordinary consumers would not understand Apple's privacy policy to include the location tracking and synching.

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.

Conclusion

As location technology becomes cheaper and more pervasive, individuals are finding that their movements can be tracked by governments and by the organizations and people in their lives. Never before has such extensive location surveillance been available. Both criminal and civil courts are preparing to set the rules for electronically tracking people, but U.S. law is a long way from settled on these matters. The business lawyer should alert clients to the practical applications of the new technology, but should warn clients that the constitutional limitations of using this technology are not clear, and that class action lawsuits may soon place limits on how the technology and the information it yields may be used by business.

Theodore F. Claypoole is a member of the Intellectual Property Practice Group at Womble Carlyle Sandridge & Rice, LLP, in Charlotte, NC. Richard C. Balough practices at Balough Law Offices, LLC, in Chicago. The authors are the co-chairs of the Mobile Commerce subcommittee of the Cyberspace Law Committee of the Business Law Section of the ABA.