Presentation to
The Nonresident Lawyers Division
Illinois Chapter of the State of Wisconsin State Bar
November 16, 2011
Chicago, Illinois

Hot Topics:

Impact of Geolocation Technologies on Privacy

Richard C. Balough

BALOUGH LAW OFFICES, LLC
1 N. LaSalle St., Ste. 1910
Chicago, IL 60602
312.499.0000
rbalough@balough.com
www.balough.com

Impact of Geolocational Technologies on Privacy

Is there any expectation of location privacy today? If you came here today and used the tollway, your I-Pass recorded the time you passed each toll, from which one can calculate your speed. If you came via the CTA and used your Chicago Plus card, it recorded the station (or bus) you entered and the time, and a camera caught your presence on the bus or station platform. The city maintains police cameras at many intersections. Private security cameras also record your movements. Face recognition software can take the images from the cameras and identify individuals. Your cell phone reports your location. If you use a discount card at the grocery store, your purchases are recorded along with the identifying information you provided.

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. The City of Chicago will offer a "Windy City Badge" to foursquare users that check in at five of 20 locations selected by the Department of Cultural Affairs and Special Events. Facebook and LinkedIn users frequently notify their friends of their location or when they leave on trips.

ComEd is installing Smart Meters that can monitor your electric usage in your home. Not only can the meters show on a real time basis the amount of electricity being used, but they also can tell the utility and others what appliances you are using and, as recently reported, can determine what television programs you watch. Smart appliances, such as a refrigerator, can tell the utility or an appliance repairman what you have in your refrigerator by using RFID chips or bar codes on your food and medicine.

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.

[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).

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 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.

The 1970 Illinois Constitution Art. 1 Sec. 6 grants Illinois citizens "the right to be secure in their persons, houses and other possessions against . . . invasions of privacy. . ." Prior to the specific Illinois Constitution language, the Illinois Supreme Court recognized the right of privacy as:

> a right many years ago described in a limited fashion by Judge Cooley with utter simplicity as the 'right to be let alone.' Privacy is one of the sensitive and necessary human values and undeniably there are circumstances under which it should enjoy the protection of law.

Leopold v. Levin, 45 Ill. 2d 434, 440 (1970). Nathan Leopold, Jr. brought suit for violation of his privacy for the distribution of a novel and related motion picture "Compulsion," which were based on the kidnapping and murder of Bobby Franks for which Leopold and Richard Loeb pled guilty in 1924. Advertisements for the book and movie used Leopold's name, and Leopold argued that the commercial use of his name constituted an invasion of privacy and an exploitation of his name. The court rejected Leopold's claim for privacy given the public figure aspect of his crime. More importantly, the court recognized the right of privacy as existing in Illinois. The court then listed the considerations for whether a right of privacy should be found to exist in a particular situation: the liberty of expression constitutionally assured in a matter of public interest, the enduring public attention to the crime, and the continuing status as a public figure. *Id.* In other words, the court applied a balancing test of the conflicting right of the public to know and the right of an individual to privacy.

Illinois recognizes a right to maintain private facts if the revelation of the facts would be highly offensive to a reasonable person and is not of legitimate concern to the public. In considering what is of legitimate concern to the public, the courts look to the "customs and conventions of the community; and in the last analysis what is proper becomes a matter of the community mores." *Green v. Chicago Tribune Company*, 286 Ill. App. 3d 1, 10 (1st Dist. 1996). If the community is an online community where the members routinely share their location, then does the use and publicizing of a member's location become an accepted norm for the community? Or can a person

share his or her location as part of an online community but not give consent to others to publicize that information. In *Ainsworth v. Century Supply Co.*, 295 Ill. App. 3d 644 (1998), the court found that giving permission for one purpose does not prevent a person from denying permission for another purpose. And where a person has a reasonable expectation that conversations would remain private, there can be an intrusion on a person's seclusion. *Johnson v. K Mart Corp.*, 311 Ill. App. 3d 573 (1st Dist. 2000). However, an Illinois court also has found no intrusion upon seclusion where a neighbor focused a camera on the plaintiff's garage entrance and recorded 24 hours a day, finding that the "complaint does not explain why a passerby on the street or a roofer or a tree trimmer could not see what the camera saw, only from a different angle." *Schiller v. Mitchell*, 357 Ill. App. 3d 435, 441 (2d Dist. 2005). Whether the court in *Schiller* would rule differently if, rather than a stationary camera, the device tracked the neighbor 24 hours a day wherever he or she went remains an issue for a future case.