GEOLOCATION PRIVACY

Implications of Evolving Expectations in the United States

KEVIN POMFRET
CENTRE FOR SPATIAL LAW AND POLICY

The concept of what constitutes "a reasonable expectation of privacy" from a geolocation standpoint is evolving in the United States. This change is not taking place in a vacuum. Rather, it directly results from growing concerns shared by the public, regulators, and lawmakers about the implications of a "Big Data" society. These concerns are fueled by a media that highlights any privacy risk associated with a new technology, regardless of its likelihood. The result will have a significant effect on organizations that collect, analyze, visualize, study, and distribute geospatial information as such information has not historically been subject to much, if any, oversight.

Ingo Baumann is co-founder and partner of BHO Legal in Cologne, Germany, a boutique law firm for European high technology projects mainly in the space sector. Ingo studied law at the Universities of Muenster and Cologne. His doctoral thesis, written at the Institute for Air and Space Law in Cologne, examined the international and European law of satellite communications. Baumann worked several years for the German Aerospace Centre (DLR), including as head of the DLR Galileo Project Office and CEO of the DLR operating company for the German Galileo Control Center.

Reasonable Expectations of Privacy and a discussion of privacy in the United States typically begins with the Fourth Amendment of the U.S. Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." In U.S. v Katz, the U.S. Supreme Court found that this Fourth Amendment protection created an individual's constitutional right to privacy.

Justice Harlan's concurrent opinion in Katz set forth what has come to be known as the "reasonable expectation of privacy" test to determine whether an individual's privacy has been violated. The test consists of two prongs. First, the judicial system must determine whether an individual has exhibited an expectation of privacy. This is the objective component of the test. The second component is subjective: assessing whether society is prepared to recognize such an expectation as "reasonable." A person satisfies both prongs if he or she has taken steps to show an expectation of privacy, and if society recognizes those expectations as reasonable under the circumstances.

Although the privacy protections of the Fourth Amendment are only applicable to the federal government, the concept is often more broadly applied to include commercial settings. For example, the legal system has generally believed that individuals do not have a reasonable expectation of privacy when in public.

This belief is based in part upon two 1986 U.S. Supreme Court decisions involving remote sensing technology. In Dow Chemical Co. v U.S, the court found that the Environmental Protection Agency (EPA) did not violate Dow Chemical's Fourth Amendment rights when it used an airplane, without obtaining a warrant, to collect aerial photographs to inspect the company's premises under the Clean Air Act. The court found that the EPA did not infringe either prong of the "reasonable

expectation of privacy" test when it flew over the company's property — even though the property was surrounded by a fence. Similarly, in California v Ciraolo, the Supreme Court ruled that the data obtained from a plane hired by the police to fly over a private home, again without a warrant, could be used in a trial.

The geospatial community has relied upon Dow Chemical and its progeny to support the position that the use of remote sensing technology to collect data of public spaces is generally immune from privacy concerns. However, several recent developments in the United States suggest that the courts, policy makers, regulators, and the public are beginning to believe that some expectation of privacy in public *are* reasonable.

An example is the Supreme Court's decision in U.S. v Jones. In Jones, the Supreme Court was asked to decide whether law enforcement was required to obtain a warrant before using a tracking device — in this case, a GPS receiver and cellular modem combination — to monitor an individual's movements in public. The Supreme Court found that the act of placing a device on an automobile without a warrant was a violation of the suspect's Fourth Amendment rights under what many considered to be an archaic theory of trespass.

In their concurring and dissenting opinions, however, a majority of the justices also appeared to suggest that long-term tracking of an individual's movements in public can violate Fourth Amendment rights. This concept, generally referred to as the "mosaic theory," suggests that continuous government collection of information about an individual could infringe on that person's reasonable expectation of privacy.

As a leading source of positioning data, GNSS — operating alone and in combination with other geolocation technologies — will figure prominently in many privacy-related legal matters.

Remote Sensing Technology

Privacy concerns associated with remote sensing data were further highlighted in a May 2014 White House report, titled "Big Data: A Technological Perspective" (the "Big Data Report'). The report was prepared by the President's Council of Advisors on Science and Technology, a group of leading scientists and engineers who make policy recommendations to the president on important technology issues. One of the topics addressed in the report was the privacy risk associated with "born analog" data – i.e., digitized information originally created in a non-digital format arising "from the characteristics of the physical world" that becomes accessible electronically when it "impinges upon a 'sensor.'"

According to the Big Data Report, one of the privacy concerns associated with "born-analog datasets is that they "likely contain more information than the minimum necessary for their immediate purpose." ("Data minimization" — collecting the minimum amount of information required to perform the task at hand — is one of the tenets of privacy protection around the world.) While the report acknowledges that a number of technological and business reasons exists for such collection to occur, the authors suggest that inherent privacy risks arise with such an approach. For example, "[a] consequence is that born-analog data will often contain information that was not originally expected. Unexpected information could in many cases lead to unanticipated beneficial products and services, but it could also give opportunities for unanticipated misuse."

The Big Data Report describes various types of "personal information" created by born-analog data. Many types of such data are quite familiar to the remote-sensing community, including "(i) video from . . . overhead drones; (ii) imaging infrared video; and (iii) synthetic aperture radar (SAR)".

The report also identifies privacy risks associated with LIDAR. While acknowledging that the technology is important to governments, industry, and a broad range of academic disciplines, the report notes that"[s]cene extraction is an example of inadvertent capture of personal information and can be used for data fusion to reveal personal information."

Drones

In addition to remote sensing, the Big Data Report cites privacy risks associated with "precise geolocation in imagery from satellites and drones," also known as unmanned aerial systems (UAS). The advent of UAS or drones prompted changes in perception about a person's reasonable expectation of privacy while in public. For example, several states have passed legislation that restricts the use of drones to collect information about an individual on private property, even if the same information could be collected by a manned aircraft.

Many of these restrictions apply to the use of drones by state agencies for law enforcement. However, others pertain to private use of drones, including by commercial entities. At the federal level, the National Telecommunications and Information Administration (NTIA) brought together stakeholders from the industry, academia, and civil rights organizations to develop voluntary "best practices" for commercial use of drones. These best practices restrict the collection of high resolution images capable of identifying an individual

A majority of the justices appeared to suggest that **long-term tracking of an individual's movements** in public can violate Fourth Amendment rights.

while in public without an individual's permission.

While the NTIA's best practices are voluntary, and apply solely to drones, we might reasonably expect that privacy proponents soon will push the concept to other remote sensing platforms. For example, the NTIA has conducted a similar multi-stakeholder initiative for facial recognition technology. More recently, the American Civil Liberties Union ("ACLU") released imagery collected by the FBI from manned aircraft of protestors in Baltimore in 2015. (The imagery had been obtained by the ACLU under Freedom of Information Act requests.)

We should expect privacy advocates to begin to argue that such imagery highlights the fact that manned aircraft are capable of creating many of the same type of privacy risks as drones and should be subject to similar restrictions. Members of the legal community have also begun to discuss whether privacy restrictions should apply to satellites. In fact, the International Bar Association recently proposed a Convention on Geoinformation that would affect all types of remote sensing activities.

Personally Identifiable Information & Data Fusion

Personally identifiable information (PII) is generally defined as information that can be used to identify an individual, either on its own or when combined with other information. Such PII as social security numbers, credit card information, email addresses, and health records have been subject to regulatory and legal protection in the United States for some time.

Until recently, geoinformation has been immune from such oversight. However, this is beginning to change as the privacy community begins to recognize the power of aggregating location with other non-PII to identify an individual. The pressure to regulate geoinformation will grow as technology makes it simpler and cheaper to aggregate and visualize it with other types of Big Data.

For example, one of the increased concerns that the Big Data Report cites is the increased power of data fusion in connection with born-analog data. Data fusion is the concept of aggregating a variety of data sets in order to develop correlations and to create profiles. The concern with data fusion is that otherwise anonymous information can be used to create a profile so unique that it can be used to identify an individual with a high degree of accuracy. To quote from the report:

> "Data fusion occurs when data from different sources are brought into contact and new facts emerge (See section 3.2.2). Individually, each data source may have a specific limited purpose. Their combination, however, may uncover new meanings. In particular, data fusion can result in the identification of individual people, the creation of profiles of an individual and the tracking of an individual's activities. More broadly, data analytics discovers patterns and correlations in large corpuses of data, using increasingly powerful statistical algorithms. If those data include personal data, the inferences flowing from data analytics may then be mapped backed to inferences, both certain and uncertain about individuals."

The privacy risks associated with data fusion should be of particular concern to the geospatial community, as lawmakers, policymakers and courts are starting to realize the power of location. For example, a number of states now restrict the collection of a zip code at the point of sale in a credit card transaction because the information can be aggregated to identify an individual without his or her consent. Similarly, the Children's Online Privacy Protection Act (COPPA) was amended in 2013 to require parental consent before collecting "geolocation information sufficient to identify street name and name of a city or town."

In June 2016, the Federal Trade Commission (FTC), settled with the mobile advertising network inMobi for collecting geolocation information on consumers without their consent. This information was obtained by geocoding a consumer's location using Wi-Fi hotspots that inMobi had mapped. A blog post on the FTC website explained that this allowed inMobi to "infer and track location without consent and regardless of a consumer's location setting."

The geospatial community **should prepare for more scrutiny in the United States** about how geoinformation is collected and used.

Consequences for the Geospatial Community

It would be a mistake to dismiss these matters as isolated events. Rather, due to the courts', lawmakers', and citizens' increasing concerns about privacy in a digital world, such legal and regulatory developments reflect a larger, global trend that is affecting a wide range of technology platforms. The change is already affecting organizations that are tapping into the power of location for a wide range of applications. For example, law enforcement's use of cellphone tracking technology has been challenged in the courts on a number of occasions. While the government has prevailed in several of these cases, they have lost others involving the use of stingray tech-

nology, which spoofs cell phone towers in order to track an individual's mobile device

These court decisions are based upon very detailed analysis of particular sections of U.S. law and not fundamental principles of location privacy, which will make it harder for users of geoinformation to know which applications are permitted and which are barred.

Similarly, the GNSS-aided Pokemon Go app has recently raised concerns about location privacy implications. Given the game's great popularity, one can expect others to develop similar apps, with increased attention to the privacy implications. As a result, the geospatial community should prepare for more scrutiny in the United States about how geoinformation is collected and used.

Additional Resources

[1] Lewis, J. J., and L. R. Caplan, "Drones to Satellites: Should Commercial Aerial Data Collection Regulations Differ by Altitude?" *GovCon Insider,* September 1, 2015

[2] Meyer, R., "This Very Common Cellphone Surveillance Still Doesn't Require a Warrant," *The Atlantic* (online), April 14, 2016

[3] Office of U.S. Senator Al Franken, "Sen. Franken Presses Makers of 'Pokemon GO' Smartphone App Over Privacy Concerns," press release, July 12, 2016 [accessed at <https://www.franken.senate.gov/?p=press_release&id=3512> August 27, 2016]

[4] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," Report to the President, May 2014[5] Rees, C., "How the IBA Is Facilitating the Development of 'Information Law,'" International Bar Association, May 16, 2013 [accessed from <http://www.ibanet.org>, August 27, 2016]

[5] *TechDirt* (online), "Maryland Court Says Cops Need Warrants To Deploy Stingray Devices," April 8, 2016 [accessed at <https://www.techdirt.com/articles/20160331/08022834061> on August 27, 2016]

[6] Wessler, N. F., and N. Dwork, "FBI Releases Secret Spy Plane Footage From Freddie Gray Protests," American Civil Liberties Union, Speak Freely blog, August 4, 2016 [accessed at <https://www.aclu.org/blog/speak-freely> on August 27, 2016]

Author

Kevin Pomfret is the founder and executive director of the Center for Spatial Law and Policy and a partner at the Williams Mullen law firm in Virginia USA. His work focuses on the legal and policy issues associated with the collection, use, storage and distribution of geospatial information. He is a member of the U.S. Secretary of Interior's National Geospatial Advisory Committee. He obtained his bachelor's degree from Bates College (Lewiston, Maine) and his law degree from Washington and Lee University School of Law (Lexington, Virginia). IG