Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Courts Tackle Tech And Privacy Trends In Law Enforcement

By **Paul Rosen and Chris Garcia**

Paul Rosen

Chris Garcia

Law360, New York (July 18, 2017, 11:45 AM EDT) -- Technology is revolutionizing police surveillance. Unlike what was portrayed in movies of years past, police are no longer reliant on stakeouts and tailing suspects to catch criminals. In the digital era, they're using smartphones and interconnected technologies to expand their reach in their investigations — and the courts are grappling with what it means for privacy and our constitutional rights.

Technology is making it easier for law enforcement to track suspected criminals, locate fugitives, biometrically identify people, search call or text records, and more. Many argue that the increasing ability of agencies to access technology records is a good thing for public safety: The easier it is for the police to take a dangerous person off the street, the better off the community. Others, however, say that precisely because technology makes it so much easier for law enforcement to obtain troves of increasingly private and personal information, the bar should be higher to do so, i.e., government should be required to obtain a warrant from a judge. This debate is playing out in Congress, in law enforcement agencies, and in courts across the country.

Warrantless Searches of Historical Cellphone Data

Last month, in granting certiorari in Carpenter v. United States, the U.S. Supreme Court reminded us that, as technology allows law enforcement to gather vast amounts of personal information from smartphones and other electronic devices, traditional standards and interpretations may not apply. This case is but the latest in a series, in which the court is re-evaluating the relationship between technology and privacy on a large scale. Its decision in this case and others could have a fundamental effect on both individuals and businesses for years to come.

In Carpenter, the Supreme Court agreed to consider whether the warrantless seizure and search of historical cellphone records revealing the location and movements of a cellphone user over the course of 127 days is permitted by the Fourth Amendment, i.e., whether law enforcement agencies must obtain warrants for such data. The case is not about real-time tracking, which generally requires a probable cause-based warrant. It is also not about the content of communications. Rather, what is at issue in Carpenter is whether law enforcement can be permitted to meet a much lower standard than probable

cause in order to require mobile phone providers to hand over historical data about where a subscriber has continuously been, every second of every day, over a period of several months.

As currently interpreted, the 30-year-old Stored Communications Act permits the government to apply to a federal court for an order directing a telecommunications provider to disclose historical cell site, or location-based information for a particular subscriber or mobile phone user. Courts have generally held that third-party wireless phone companies collect such data in the ordinary course of business, and subscribers who have voluntarily provided it have no reasonable expectation of privacy in that information. Therefore, no warrant is required. Rather, the governing statute requires the government to demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation."

In Carpenter, the government did just that. The case involves a string of armed robberies of, coincidentally, cellphone stores spanning a two-year period. One of the defendants confessed to the crime and gave the mobile phone numbers of his co-conspirators to the government. The government then applied for court orders for the cell-site records of each number, including defendant Carpenter's.

The government's application was granted, and it received 127 days of historical cell-site records associated with Carpenter's mobile number; that is, his approximate location for the entire time period. This information placed Carpenter's phone near the robberies at the time they took place. Carpenter was ultimately convicted for the robberies and appealed.

Carpenter has important implications for law enforcement and investigative targets. If the Supreme Court decides that the government must obtain a probable cause-based warrant, fewer disclosure orders will be issued, and it will be harder for prosecutors to prove cases, particularly those where they are trying to put defendants at the scene of a crime. Prosecutors will need to gather more evidence, such as a witness statement, to show there is probable cause to believe that the location information will show evidence of criminal activity.

It also has implications for businesses. For example, companies generally freely determine how long to retain subscriber records. Depending on their business models and goals, companies may vary their retention policies as courts continue to interpret the scope of individual privacy rights in possession of third parties. If the Supreme Court decides that greater protections are required for historical location-based data and moves in the direction of a warrant, it may also affect the manner in which companies develop products with advanced tracking technologies.

In many ways, however, the reasoning behind the Supreme Court's decision will be more important than its ultimate conclusion. The holding may, for the first time with the current court composition, provide its latest view on the government's authority in the digital age and its impact on privacy. It may also revisit the longstanding "third party doctrine" and weigh in on whether an individual's provision of detailed personal information to third parties, e.g., telecommunications providers, is truly voluntary and therefore without any reasonable expectation of privacy.

This is not the first case where the court will address the government's power in light of great advances in technology.

Cellphone Searches at Arrest Require a Warrant

In 2014 in Riley v. California, a unanimous Supreme Court disturbed years of precedent to hold that

searching an arrestee's cellphone required a warrant. Historically, a search of a person and the areas into which he or she may reach were deemed searches incident to an arrest, not requiring a separate warrant. The reasoning in Riley was telling: Chief Justice John Roberts wrote, "Modern cellphones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"

In the wake of Riley, Carpenter poses an interesting question: If the Supreme Court believes that access to information on a cellphone should generally require a warrant, would that same rationale apply to historical, location-based data? Or will the third-party doctrine, which Justice Sonia Sotomayor has called "ill-suited to the digital age," change the analysis?

The answer will not only impact investigators and criminal lawyers. It will also cause businesses to rethink how they collect and store all sorts of information that they hold as third parties, from call and text records to bank and payment information and more.

Real-Time Tracking Devices Require Warrants

In the context of modern technology, the Supreme Court has been drawing distinctions from traditional doctrines that may once have permitted similar warrantless searches or seizures. Shortly before Riley, in 2012, the Supreme Court held that the government must obtain a warrant to place a tracking device on a vehicle, even if parked in a public lot.

In United States v. Jones, police were investigating a suspected drug trafficker and placed a GPS device on his car. The Supreme Court unanimously held that the installation of the GPS device was a search under the Fourth Amendment. Before Jones, the government relied on Supreme Court precedent that movement on a public road was not protected Fourth Amendment activity since a person has no reasonable expectation of privacy in actions made known to the general public. At oral argument, Justice Samuel Alito set down a marker for the court's thinking in remarking that, "Technology is changing people's expectations of privacy."

The question the Supreme Court and lower courts across the country seem to be grappling with is whether an individual's reasonable expectation of privacy is any different in light of the intrusive capabilities that emerging technology offers. New technologies, such as drones and self-driving automobiles, will bring these questions to the forefront, and the forthcoming Carpenter decision may very well begin to answer some of these questions.

Federal Agencies Get Proactive

Courts are not the only institutions recognizing the role technology plays in our lives and how it affects privacy. In 2015, the U.S. Departments of Justice and Homeland Security — within which exist the major federal criminal investigative agencies — took a voluntary step of issuing policy guidance that required investigators and prosecutors to obtain a search warrant before deploying cell-site simulator technology.

The simulator — which is a device often affixed to a moving vehicle — allows law enforcement to locate wanted individuals or victims by transmitting as a cell tower and tricking devices in the vicinity to connect to the mobile cell site, thereby allowing law enforcement to locate the device (and its user), or identify a previously unknown device of an investigative subject. Similar to the Carpenter situation, generally all that was required to deploy the simulator was a court order pursuant to the Pen Register Statute.

The move by the DOJ and DHS indicated that the agencies recognize the privacy implications of some of their investigative tools, and are willing to take measures to get ahead of courts prescribing a particular standard. It also showed the impact that Congress and nongovernmental privacy organizations — two constituencies that raised questions about law enforcement's warrantless use of cell-site simulators — have in shaping policy in this area.

Increased Warrantless Searches at the Border

Finally, federal authorities' searches of electronic devices at international borders and the courts' responses are also raising questions about how intrusive the government may be when it comes to accessing data in advanced technologies. Courts have long held that the government can freely search international travelers and their belongings at an international border (including an international airport) without a warrant. And customs officials are doing just that.

The number of warrantless border searches by customs officials has recently doubled to nearly 15,000 in the first six months of fiscal year 2017. But as these searches increasingly affect the trove of private information stored on smartphones and computers, courts have begun weighing in on this long-standing principle.

In 2013, the Ninth Circuit determined that reasonable suspicion was required to conduct a forensic laptop search of an international traveler because of the "uniquely sensitive nature of data on electronic devices." In 2015, a federal district judge in Washington, D.C., relying on Riley, held in United States v. Kim that computer searches at the border must be "reasonable" under the totality of the circumstances, in part because the search was "so invasive of [the defendant's] privacy."

Looking Ahead in the Courts

In all of these areas, courts are just beginning to tackle the legal implications of emerging technology, which is only going to become a more complex exercise as technology developments race forward. Whether it is cell-site simulators, GPS devices, location data from cellphones and other "smart devices," or something entirely new — such as self-driving cars — all of these increasingly connected technologies are playing a profound role in shaping how courts and regulators view privacy.

What makes today's technological revolution different is the ubiquity of its availability; it seems safe to speculate that every justice on the Supreme Court has a mobile phone, as does every government regulator and member of Congress. They, like most Americans, keep their phones with them at all times, making their every movement potentially subject to government review. The justices have a sense of what they expect to be private and what law enforcement should have to show before that information is divulged to the government — and we will continue to see this reflected in their jurisprudence.

The outcomes of cases such as Carpenter will have a significant impact in the areas of criminal law and technology policy, and provide a good sense of where the new court will take these long-standing legal doctrines in the digital age.

What is certain is that law enforcement agencies will continue to find new ways to leverage technology for investigations, and the courts will continue to face a new age of pivotal privacy and data security cases that will have a lasting impact on law enforcement and the privacy of all Americans.

In the wake of these developments, company executives must be engaged early and often —

understanding how their products are being developed and how their technology is being used. At the same time, businesses need to understand how their technology affects (for better or worse) investigations so they can appropriately craft privacy and data retention policies, send their employees on international travel with sensitive business information, and respond to government inquiries and investigations. In the end, we will continue to live in a country where the courts and American people strike a balance between giving government the important tools it needs to keep communities safe and ensuring individual privacy protections continue to thrive.

Paul Rosen is a partner in the Los Angeles and Washington, D.C., offices of Crowell & Moring LLP and a former federal prosecutor. He was the chief of staff at the U.S. Department of Homeland Security until January 2017. He is also a nonresident fellow at Harvard's Kennedy School of Government, Homeland Security Project.

Christopher D. Garcia is an associate in the firm's Los Angeles office.