Department of Justice

STATEMENT OF

RICHARD W. DOWNING
ACTING DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"GEOLOCATION TECHNOLOGY AND PRIVACY"

PRESENTED

MARCH 2, 2016

Richard W. Downing
Acting Deputy Assistant Attorney General
Department of Justice

Before the
Committee on Oversight and Government Reform
U.S. House of Representatives

At a Hearing Entitled
"Geolocation Technology and Privacy"

Presented
March 2, 2016

Good morning, Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the topic of geolocation information. The Department recognizes the importance of considering individual privacy interests when obtaining different types of geolocation information. At the same time, location information often plays an important and sometimes pivotal role in our efforts to protect public safety and seek justice. I will discuss some of the types of location information that Federal law enforcement investigators obtain, the types of legal authorization utilized to do so, and the standards that we must meet in order to obtain that legal authorization.

"Geolocation information" is not a single kind of information, nor is there one agreed-upon definition. Law enforcement uses a variety of different kinds of location information that provide some indication of the location of a particular person or thing. Depending on what type of location information is at issue, such information has different evidentiary significance, and how it is accessed implicates very different privacy concerns and legal provisions.

Location information can differ in how precisely the data can identify location, from the most general, such as the country in which someone or something is located, to the quite specific, such as measurements of latitude and longitude generated by a GPS system. Information concerning the location of a person or a thing is sometimes gathered directly by law enforcement officers, such as through the use of cell site simulators. In other circumstances, officers obtain location information from cell phone carriers and other commercial entities. These companies sometimes collect location information for their own business purposes, such as to improve their networks or target advertising, and at other times only in response to a warrant or order issued by a court. Some types of location information are collected continuously, while other types are collected only periodically or in connection with a specific transaction or event.

Let me provide some examples of how location information can be critical to solving crimes, protecting public safety, and seeking justice.

In one case, after a U.S. District Court judge in Jacksonville, Florida, was shot at with a high-powered rifle while he sat in his living room – and, thankfully, was not seriously harmed – investigating agents were faced with a very large pool of potential suspects, including many defendants and litigants who had appeared before that judge. Agents were able to use court orders issued under section 2703(d) of the Electronic Communications Privacy Act to obtain cell-site records that significantly narrowed the list of potential suspects. This advanced the investigation and conserved investigative resources by allowing agents to exclude certain potential suspects and pursue leads that eventually led to the arrest of the alleged shooter.

Another example concerns the fatal shooting of two students at the University of Southern California while they were parked in a vehicle near campus in 2012. The subjects stole the victims' cell phones. Ballistics evidence tied the shooting to another shooting earlier that year, causing investigators to focus on two suspects. The suspects' phone records, including historical cell-site information, were obtained with the State equivalent of a 2703(d) order. The location information showed that the suspects were in the vicinity of the crime scene at the time of the shooting, and they also showed that the suspects' phones were in the same vicinity as the victims' phones after the homicide. This information was critical to developing additional evidence supporting the murder prosecutions against the suspects. They were charged and convicted and are both serving sentences of life in prison without the possibility of parole.

Although it would be impossible to discuss in detail all of the varying types of location information, I would like to describe several categories of such information and the legal authority that typically is required to obtain that information. I will start with more precise location information carrying stronger privacy interests and which, because of constitutional or statutory requirements or Department policy, require a higher legal showing to obtain.

GPS and Similar Location Information from Wireless Carriers

Some carriers have the ability to determine the location of a user's wireless device by relying on the device's built-in GPS capability. Other carriers do not rely on GPS, but have similar capabilities to locate a device by measuring signals the device sends to multiple towers or other antennas. The FCC has mandated that all carriers have this capability so that emergency responders can find the device when the user dials 911. Using such techniques, a carrier can determine fairly precisely the phone's location and can do so nearly continuously. Such location information is generally only created when the user dials 911 or when the carrier receives legal process.

To obtain this information on a prospective basis from a wireless carrier, officers generally obtain a search warrant from a court based on probable cause. Exceptions to this rule include special situations such as where the phone user has consented or where there is a life-and-death emergency. Our experience has been that such information about the precise location of a device is not generally available on a historical basis from wireless carriers because such

companies do not maintain such information in the ordinary course of business and without specific court authorization requiring it.

Use of Cell-Site Simulators

Cell-site simulators are devices operated by law enforcement officers that can help determine the location of a known cellular device. The technology works by collecting a limited set of signaling information from cellular devices in the vicinity of the simulator in order to find the relative signal strength and general direction of a particular cellular telephone. Cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication.

In September 2015, the Department issued a new policy governing its use of cell-site simulators in domestic criminal investigations. The policy is intended to enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections.

The policy adopts a consistent legal standard for the Department's use of cell-site simulators in domestic criminal investigations. While the Department has, in the past, obtained appropriate legal authorization to use cell-site simulators pursuant to orders under the Pen Register Statute, law enforcement agents now are required to obtain a search warrant supported by probable cause before using such a device. The policy recognizes that there are limited exceptions to the warrant requirement, such as exigent circumstances.

Tracking Devices

Another type of device operated by law enforcement that can provide information about the location of a person or object is a tracking device. In *United States v. Jones*, the Supreme Court held that the warrantless installation of a tracking device on a target's vehicle, and the use of that device to monitor the location of the vehicle over a 28-day period, constituted a search within the meaning of the Fourth Amendment. In light of the *Jones* decision, law enforcement agents now generally obtain a search warrant supported by probable cause before the installation and monitoring of a tracking device on a vehicle. There are, however, circumstances including long-standing exceptions to the warrant requirement, such as consent or exigent circumstances, where a warrant would not be required.

Cell-Site Information

Another category of location information is called cell-site (or cell tower) information. Cell-site information consists of business records that wireless carriers routinely collect and maintain as part of the service they provide to customers. This type of data generally provides less exact and less detailed information about a device's location than the GPS and similar information discussed above.

Cellular devices operate through radio communications with a carrier's cell towers. When a user places or receives a call, or sends or receives a text or data message, the device sends signals to a cell tower. Most towers divide their coverage area into three roughly pie-shaped "sectors", each of which corresponds to a separate antenna (or "face") that receives signals from wireless devices. Because each tower does not have unlimited range, the fact that a particular tower and sector handled some or all of a communication gives a rough idea of the location of the device at the time that the communication occurred. The service area of the tower can vary widely, depending on such factors as local topography, network traffic, and whether it serves a rural or urban area.

The records of the towers and sectors handling communications with a particular device are called cell-site information. Carriers have discretion over what types of cell-site information they choose to record and keep and how long they keep it. Carriers generally keep cell-site information related to phone calls; some also keep records related to text messages or certain data transfers. We are not aware of any carrier that keeps records of cell-site information for every signal sent between a device and towers. Carriers usually keep cell-site records for at least six months. Courts can compel the disclosure of historical cell-site information (*i.e.*, the tower/sector records made by the carrier regarding calls or text messages sent or received by the user in the past). They can also compel the disclosure of similar information on an ongoing basis.

Historical cell-site information by definition does not provide the location of the device in real-time. Providers, in their ordinary course of business, collect and maintain records of which towers devices use for their own purposes. Carriers use this information to repair and improve their networks so that, for instance, customers have fewer dropped calls and faster downloads. In addition to being generally less precise than GPS or similar information, this data is collected by the provider only periodically.

The Electronic Communications Privacy Act allows a government entity to compel disclosure of historical cell-site records via a court order issued on a finding of "specific and articulable facts" that the records sought are relevant and material to an ongoing criminal investigation. These orders, often called 2703(d) orders, provide more privacy protection than a standard subpoena by mandating prior judicial review and requiring a higher evidentiary threshold than the traditional relevance standard for subpoenas. Most Federal courts that have considered the issue – including three circuit courts and more than twenty district courts – have held that the wireless carriers' historical business records about network activity are properly obtained with a court order under section 2703(d) of the Electronic Communications Privacy Act.[1]

[1]A handful of lower courts have held that a search warrant was required to obtain historical cell-site records. A panel of the Court of Appeals for the Fourth Circuit had held that a

Prospective cell-site records are similar to historical cell-site records except that a provider discloses the records to law enforcement on an ongoing basis. In normal circumstances, for the Department to obtain this information, at a minimum a court must issue an order based on a finding that the request has satisfied both the requirements of the Pen Register Statute and the requirements for a court order under section 2703(d) of the Electronic Communications Privacy Act. Some courts have required a search warrant.

Other Business Records from Which Location May Be Inferred

Finally, there are a variety of other types of records from which investigators and fact-finders may infer the location of a person or a thing at a particular time. For example, when someone withdraws money from an ATM, uses a credit card at a store, or pays a bridge toll, businesses generate records that, among other things, suggest that the customer was at a specific place at a specific time. The customer voluntarily conveys to the business the identity of her card or device, and the business commonly makes a record of the information along with the location of the transaction. Such records are generally generated by the business only as often as the transaction occurs.

Many of these records of business activities do not include providing customers with communication services and therefore are not covered by the Electronic Communications Privacy Act, and some of them are not covered by any statute. In line with longstanding Supreme Court precedent governing how the Government may obtain third-party business records, the Department generally relies upon subpoenas to compel disclosure of such records.

Conclusion

Given the wide variety of different types of information that provide some indication of the location of a particular person or thing—as well as the different ways in which this information is generated and maintained, the different levels of precision it offers, the different ways that such information can be accessed, and the different privacy implications – it is appropriate that the law provide a variety of mechanisms for law enforcement to acquire such information. The Department is dedicated to ensuring that its policies and practices comply with those laws and enable law enforcement officers to seek justice and protect public safety while continuing to uphold the Department's long-standing commitment to promoting individuals' privacy and civil liberties. We are pleased to engage with the Committee in a discussion about this important issue.

---

search warrant is required to obtain historical cell-site location; however, that panel decision was vacated and will be heard by the full Court soon.

RICHARD W. DOWNING
Deputy Assistant Attorney General (Acting)

Richard W. Downing was selected to serve as Acting Deputy Assistant Attorney General for the Criminal Division at the Department of Justice, in September 2015. Mr. Downing previously served as Principal Deputy Chief of the Computer Crime and Intellectual Property Section. During his tenure, he supervised the prosecution of hacking, identity theft, and intellectual property crimes, oversaw policy and litigation governing the constitutional and statutory rules for the collection of electronic evidence, and supervised the development of international law enforcement cooperation related to cybercrime and intellectual property crime.

Mr. Downing joined the Department of Justice in 1999. Prior to that, he served for seven years as an Assistant District Attorney in Philadelphia. He graduated with a J.D. from Stanford Law School in 1992 and received a B.A. in Political Science, *summa cum laude*, from Yale University in 1989.