THE NATIONAL LAW JOURNAL
JUNE 27, 2012
Online Feature
An ALM Publication

High court's GPS ruling may have minimal impact because cellphone tracking is legal

BY RICHARD Q. HARK

The U.S. Supreme Court recently held in U.S. v. Jones that the warrantless use of a government-placed GPS tracking device on a defendant's vehicle constitutes a trespass, requiring suppression of all evidence generated there from. Some thought Jones could become a significant step in Fourth Amendment jurisprudence protecting defendants' rights. However, in 2010, Congress amended the Stored Communications Act (SCA), 18 U.S.C. 2701, severely curtailing Jones' importance. This is because a vast majority of people in the United States voluntarily carry a GPS tracking device — their cellular telephone — to which the 2010 SCA amendments gave the government almost unfettered access.

The 2010 SCA amendments reflect updated government demand for advanced surveillance techniques of electronic and wire data previously unavailable to law enforcement. The SCA regulates the manner in which law enforcement can obtain data concerning private electronic and wire communications, the contents of these transmissions and other historical information electronic communication service providers must now store.

Subsections 2703(a), (b) and (c)(1) of the SCA, respectively, allow disclosure to the government of the contents of wire or electronic communications in electronic storage, the contents of wire and electronic communications held by remote computing service, and a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications).


Richard Q. Hark

The process commences with an agent's informal § 2703 request to a service provider or storage entity with regard to a specific phone number. The service provider then accumulates and holds the data for up to 180 days pending court approval, with one extension of equal time.

"Content" includes complete texts, e-mails, all attachments and time and length of all telephone calls. Government notice of a § 2703(b)(1) content request must be provided to the subscriber. Notice may be delayed or placed under seal upon a showing that an adverse result may occur. An adverse result is potential flight of, or injury to, the subscriber, evidence tampering, witness intimidation or investigatory delay.

"Other information" is historical and real time "cell site location information"; antenna towers used; the date, time and length of call; call handoffs; registrations; and connection records. This is the GPS triangulation evidences that pinpoints historical and real-time subscriber location within 50 feet of where a cellular phone call was made or received or smartphone Internet usage triggered.

The different ways the government may obtain § 2703(a), (b) and (c) data are significant. A warrant is required for § 2703(a) current content from an electronic communications system or its storage. Content older than 180 days may be applied for consistent with § 2703(b).

Section § 2703(b) and (c) allow for access via judicial warrant based upon probable cause; subscriber or customer consent; information subpoena; court order for such disclosure under subsection § 2703(d); and a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address and place of business of a subscriber or customer of such provider, who is engaged in telemarketing (as such term is defined in § 2325 of this title). The subpoena option reveals basic customer identity and means of payment, not cell site location information. All § 2703(b) and (c) information is sought ex parte, under seal, and no notice to the consumer is required.

The heart of the 2010 SCA amendments is § 2703(d), which authorizes government application for historical and current content and cell site location information without a warrant or subpoena. This provision requires a court order for access to certain content and all cell site location information. A magistrate judge shall issue the order "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other infor-

mation sought, are relevant and material to an ongoing criminal investigation." The § 2703(d) application is filed ex parte and under seal. It is for the magistrate judge to ensure that the government has met its limited burden of proof of "specific articulable facts that [cell site location information] is relevant and material to an ongoing criminal investigation." Typically, judicial deference to the case agent's opinion as to materiality, without a hearing, occurs.

In In re Application, 620 F.3d 304 (3d Cir. 2010), the U.S. Court of Appeals for the Third Circuit became the first appellate court to review a magistrate judge's denial of a § 2703(d) application. Prior thereto, numerous district courts addressed various issues regarding government access to prospective cell site location information through § 2703(d) alone or in a hybrid application utilizing pen register and trace-and-trap statutes. Procedurally, the magistrate judge, joined by several colleagues, held that the probable-cause standard applied and denied the government's application. The government appealed, and the district court affirmed. The Third Circuit reversed and remanded for a factual finding to determine if the government met its burden of proof under the lower standard.

In its reversal, the Third Circuit upheld the congressional prerogative of allowing ex parte government access to historical and prospective cell site location information, of which privacy interests exist, based upon the mere representation of reasonable grounds to believe that cell or smartphone location is relevant and material to an ongoing criminal investigation. This standard is lower than probable cause and reasonable suspicion. Further, the court concluded that the magistrate judge must issue the order upon concluding the government met its burden of proof.

Significantly, the court understood that these data could include the whereabouts of persons in private residences not open to visual surveillance. In 1984, the Supreme Court rejected this type of information request in a "beeper" case, which also had been sought without a warrant under a standard lower than probable cause. In re Application is a primer for all issues regarding a § 2703(d) order, including the difference between wire and electronic communications, intended government use of the data for which it has applied, and the ability of magistrate judges to deny the application.

From a practice standpoint, government discovery disclosure of cell site location information and other § 2703 documents will occur only after a motion to unseal has been filed. Specific discovery requests must be made for both content and cell site location information pursuant to Federal Rule of Criminal Procedure 16 (E), (F) and (G). A motion to compel may be in order if the government provides basic cell site location information but not a written summary of any expert's testimony (including the expert's opinions, bases and reasons for those opinions, and qualifications). Counsel must establish that the information sought is material to guilt or innocence and expert testimony is necessary to secure admission into evidence the historical cell tower data.

Counsel must conduct a thorough review of each cell site location information application to each electronic communication service provided, and the exact documents disclosed. It is appropriate to file motions to preclude admission into evidence of SCA records (personal information, content and/or cell site location information) obtained incorrectly (under which § 2703 provision) or which the service provider erroneously provided. Counsel should analyze each case agent's reasonable grounds and materiality claims in the § 2703(d) applications.

Counsel should also correlate each name and address of the cellphone's subscriber to the cell site location information session time, durations and locations. In other words, counsel should correlate the defendants' or witness's locations to the specific cellphone cell site location provided. A lack of correlation because a cellphone that was lent out, stolen or lost is material to innocence or guilt. Counsel should substantiate any alibi to strengthen each factual divergence.

In addition, counsel should corroborate cell site location information and government-secured contemporaneous video surveillance. Although the data may have been collected in real time, it is provided to counsel many months after the fact. To the extent investigation reveals that contemporaneous video surveillance was available but not obtained, significant trial issues will abound. Concurrently, if street video depicts a person other than the defendant on the telephone identified at a specific location, reasonable doubt may lay.

While GPS data may be the death knell to any proposed defense, it has excluded many defendants from being included in certain types of conspiracies or superseding indictments involving copy-cat cases. It is up to counsel to understand the evidence used against a client and properly investigate the legal means by which that information was secured.

Richard Q. Hark is a partner at Hark & Hark in Philadelphia.