Study G-300 February 3, 2015

First Supplement to Memorandum 2015-3

State and Local Agency Access to Customer Information from Communication Service Providers: General Statutory Objectives

This supplement continues the discussion that was begun in Memorandum 2015-3, of the overall objectives for proposed legislation in this study.[1] It discusses location tracking.

LOCATION TRACKING

There are currently two general ways that service providers can track the location of cell phones and other mobile communication devices:

(1) *Cell tower triangulation.* Cell service providers are able to approximate the location of a cell phone, by applying a triangulation algorithm to data about its communication with nearby cell towers.[2]

(2) *Global positioning system (GPS) data.* Many cell phones and other mobile communication devices are capable of determining the precise location of the device by using the GPS satellite system.[3]

Service provider records showing a device's location are metadata, because they describe the status of the communication device, rather than the content of

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

2. Congressional Research Service, *Governmental Tracking of Cell Phones and Vehicles: The Confluence of Privacy, Technology, and Law* at 8, n.60 (2011) ("There are two distinct technologies used to locate a cell phone through a network: time difference of arrival and the angle of arrival. … The time difference technology measures the time it takes for a signal to travel from the cell phone to the tower. When multiple towers pick up this signal, an algorithm allows the network to determine the phone's latitude and longitude. … The angle of arrival technology uses the angles at which a phone's signal reaches a station. When more than one tower receives the signal, the network compares this data the multiple angles of arrival and triangulates the location of the cell phone.").

3. *Id.* ("GPS, or Global Positioning System, is a system of 24 satellites that constantly orbit Earth. … When hardware inside the cell phone receives signals from at least four of these satellites, the handset can calculate its latitude and longitude to within 10 meters.").

communications. As such, much of the constitutional analysis of government access to location tracking data is the same as that which governs access to metadata generally. In other words:

- The third party exception to the Fourth Amendment may defeat any reasonable expectation of privacy with regard to location data, taking such information out of the Fourth Amendment's protection.
- The same would not be true under the California Constitution, because there is no third party exception to Article I, Section 13 of the California Constitution.[4]

However, location data presents other special constitutional and statutory issues, which are discussed below.

The discussion that follows is focused on location information that is generated by a person's mobile communication device and collected by government from the person's communication service provider. That kind of surveillance is squarely within the scope of the current study. For ease of reference, this memorandum will use the term "cell phone tracking" to refer to that kind of surveillance (with the understanding that the term encompasses more than just cell phones).

The use of a "slap on" tracking device that is affixed directly to a vehicle or other object does not involve information obtained from a customer's communication service provider. That kind of surveillance is not within the scope of the study and is not discussed further.

Constitutional and Statutory Requirements

Fourth Amendment

In addition to the third party issue noted above, there is another reason why cell phone tracking may not be subject to the Fourth Amendment. In general, when a person moves from place to place, the person does so in public, subject to observation by any person. There is no reasonable expectation that one's public movements are private. "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[5]

4. See Memorandum 2015-3, pp. 28-29.
5. United States v. Knotts, 460 U.S. 276, 281 (1983).

However, cell phone tracking can also be used to pinpoint a person's location within *private* places, where movements are not susceptible to public observation. In those situations, there may still be an expectation of privacy that is protected by the Fourth Amendment.[6]

Notwithstanding the "public movement" issue noted above, five United States Supreme Court Justices recently suggested, in *dicta*, that cell phone tracking *could* violate the Fourth Amendment, depending on the seriousness of the crime being investigated and the duration of monitoring. The Justices suggested that cell phone tracking would be unconstitutional on the facts that were before them:

> In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.[7]

It therefore seems likely that some degree of cell phone tracking is subject to the requirements of the Fourth Amendment.

Federal Statutory Law

The *retrospective* collection of cell phone tracking information appears to be governed by the Stored Communications Act ("SCA").[8] Like other metadata, cell phone tracking information could be obtained by government through the use of a warrant or a court order issued under 18 U.S.C. § 2703(d).[9]

The federal statutory law governing *prospective* real-time cell phone tracking is not settled.[10] Some courts have held that federal statutory law does not clearly authorize prospective cell phone tracking.[11] But a few courts have accepted the

6. United States v. Karo, 468 U.S. 705, 714-15 (1984).

7. United States v. Jones, 132 S. Ct. 945, 958 (2012) (Alito, J., concurring); *id.* at 955 (Sotomayor, J. concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'").

8. See, e.g., In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

9. 18 U.S.C. § 2703(c).

10. See Memorandum 2014-33, pp. 36-38.

11. See generally Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use, 15 A.L.R. Fed. 2d 537 (2014).

argument that the SCA combined with the Pen Register Act provide a form of "hybrid" authority for prospective cell phone tracking.[12]

California Statutory Law

There is a provision in the California Invasion of Privacy Act that generally prohibits the use of an "electronic tracking device" to determine the location or movement of a person.[13] That prohibition has an exception for the lawful use of a tracking device by law enforcement.[14]

In 2012, the Legislature and Governor added Penal Code Sections 1524(a)(12) and 1534(b), which authorize the issuance of a warrant when law enforcement uses a tracking device.[15] In that context, the term "tracking device" is defined as "any electronic or mechanical device that permits the tracking of the movement of a person or object."[16] That definition is quite broad and appears to encompass tracking information generated by a mobile communication device (e.g., a cell phone) that is obtained by the government from a communication service provider. That broad reading of the provision is consistent with apparent legislative intent[17] and with express statutory language.[18]

What Level of Legal Process Should be Required?

It is very likely that the Fourth Amendment applies to cell phone tracking in at least *some* circumstances. (The same is probably true of Article I, Section 13 of the California Constitution, with the added point that there is no third party limitation on that provision).

Unfortunately, the case law does not clearly state a threshold for the application of the Fourth Amendment to cell phone tracking. The concurring Justices in *Jones* suggest that four weeks of tracking in a drug trafficking case is enough to trigger the Fourth Amendment. But it is not clear whether a shorter period of tracking would also be governed by the Fourth Amendment. Nor is it

12. *Id.*
13. Penal Code § 637.7(a).
14. *Id.* at (c).
15. See 2012 Cal. Stat. ch. 818 (AB 2055 (Fuentes)). See also Penal Code § 1534(b) (use of tracking device warrant).
16. Penal Code § 1534(b)(6).
17. See Memorandum 2014-50, pp. 19-21; Assembly Public Safety Committee Analysis of AB 2055 (April 17, 2012), p. 4 ("This bill establishes that a warrant is required to obtain tracking-device data, regardless of whether the data is collected by means of physical intrusion or mined by law enforcement through devices installed or used by the owner.").
18. Penal Code Section 1534(b)(1) ("The search warrant shall command the officer to execute the warrant by installing a tracking device *or serving a warrant on a third-party possessor of the tracking data.*") (emphasis added).

clear how the severity of the crime that is being investigated would factor into the standard for application of the Fourth Amendment.

In order to avoid any unconstitutional cell phone tracking, the proposed legislation should probably require a warrant in at least some circumstances. But it is not clear where the line should be drawn. If warrants are always required for cell phone tracking, there may be circumstances in which the statute requires more process than is needed to satisfy the Fourth Amendment. But if the statute allows some warrantless cell phone tracking, then it could produce unconstitutional results in some cases.

Importantly, California has already resolved that question. Under the statutes that were enacted in 2012, a warrant is always required for cell phone tracking. If the proposed law were to continue that existing statutory approach, there would be no risk of a Fourth Amendment violation.

Should the proposed legislation take that approach, continuing the existing California statutory rule? If not, the Commission will need to decide where to set the threshold for requiring a warrant.

Opportunities for Reform

In examining the California statutes governing the use of tracking devices, the staff discovered some apparent technical problems in Penal Code Section 637.7, which reads as follows:

> 637.7. (a) No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.
>
> (b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.
>
> (c) This section shall not apply to the lawful use of an electronic tracking device by a law enforcement agency.
>
> (d) As used in this section, "electronic tracking device" means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.
>
> (e) A violation of this section is a misdemeanor.
>
> (f) A violation of this section by a person, business, firm, company, association, partnership, or corporation licensed under Division 3 (commencing with Section 5000) of the Business and Professions Code shall constitute grounds for revocation of the license issued to that person, business, firm, company, association, partnership, or corporation, pursuant to the provisions that provide for the revocation of the license as set forth in Division 3 (commencing with Section 5000) of the Business and Professions Code.

The problems in Section 637.7, which are described below, could perhaps be addressed in the proposed legislation.

Definition of "Electronic Tracking Device"

The definition of "electronic tracking device" that is provided in Section 637.7(d) appears to be too narrow. It only includes a tracking device that is *attached* to a vehicle or moveable object. That would seem to exclude mobile phones and other portable communication devices (which are typically not "attached" to vehicles or other objects).

That narrow definition is at odds with Section 1534, which defines "tracking device" much more broadly, with the apparent intention of including a mobile communication device that is used for cell phone tracking.

In order to better coordinate the two provisions, the definition in Section 637.7(d) should probably be revised to parallel the definition used in Section 1534(b)(6), thus:

> (d) As used in this section, "~~electronic~~ tracking device" means any ~~device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals~~ electronic or mechanical device that permits the tracking of the movement of a person or object.

If that change were made, conforming changes would be needed throughout the section, to replace "electronic tracking device" with "tracking device." **Should the proposed legislation include such revisions?**

Scope of Consent Exception

If Section 637.7 is revised to broaden the definition of "electronic tracking device," as proposed above, then it would probably be necessary to broaden the scope of the consent-based exception in Section 637.7(b). In the existing provision, that exception only applies when consent is given by the owner, lessor, or lessee of a *vehicle* that is being tracked. There is currently no exception for consent given by a person whose mobile communication device is being tracked.

This could cause serious problems. There are numerous "apps" that track the location of portable communication devices, with the express consent of the owner. If the consent exception in Section 637.7(b) does not include consent given by the owner of a communication device, then routine location tracking apps could violate Section 637.7.

Should the proposed legislation revise Section 637.7(b) so that it includes the consent of the owner of any type of object that is to be tracked?

Scope of Prohibition

The prohibition in Section 637.7(a) may be too narrow. It only prohibits the use of a tracking device to determine the location or movement of a *person*.

That narrow scope is at odds with other language in Sections 637.7 and 1534 which clearly contemplates the use of a tracking device to track the movement of *objects*.

This matters because there are situations in which the location of an object might be tracked, even if it is not co-located with a particular person.

Should Section 637.7(a) be revised to include the tracking of objects as well as people?

Respectfully submitted,

Brian Hebert
Executive Director