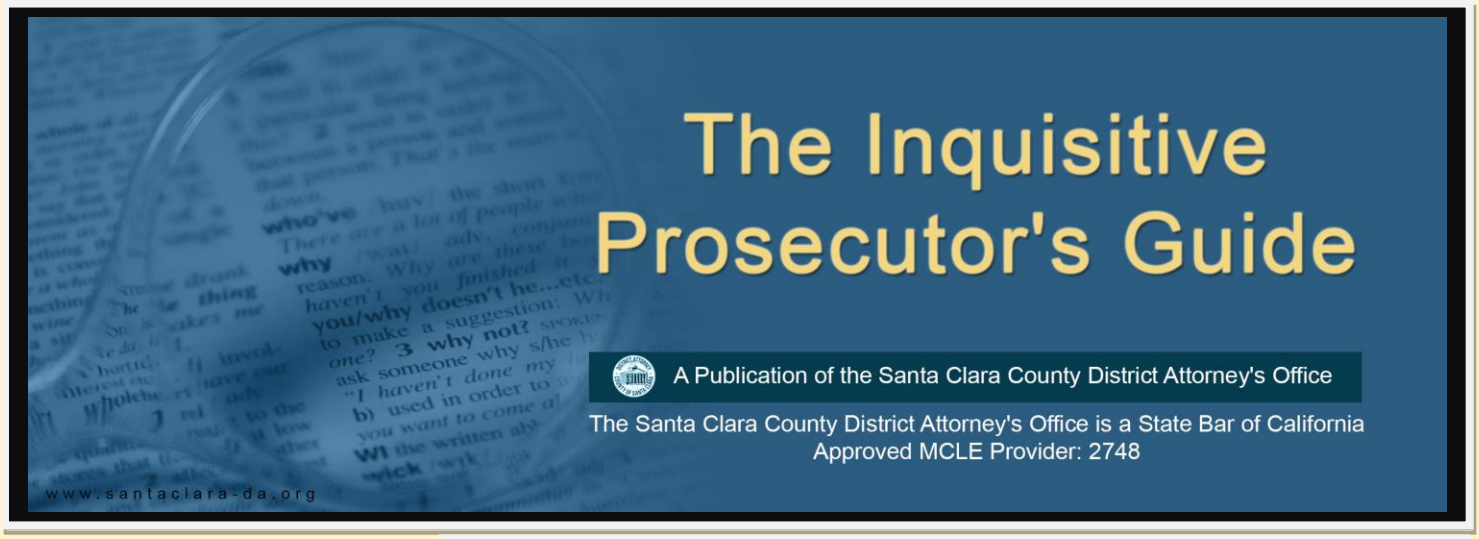

Date: August 7, 2018

2018-IPG-38 (OBTAINING CELL SITE INFO: *CARPENTER*)

In this edition of the Inquisitive Prosecutors Guide, we discuss the recent United States Supreme Court decision in ***Carpenter* v. *United States*** (2018) 138 S.Ct. 2206, a case deciding whether a warrant is required to obtain cell site location information (CSLI), and its potential impact on law enforcement's ability to obtain CSLI. Among the issues discussed:

Does this decision have any real impact on the ability of law enforcement in California to obtain CSLI without a warrant – considering that the California Electronic Communication Privacy Act already generally requires a warrant for electronic communication information?

Will this decision impact a prosecutor's ability to subpoena third party records *in general* when a defendant has a privacy interest in the third-party records?

If exigent circumstances exist, can the government obtain either historical or real-time CSLI without a warrant?

Note: If you only have 15 seconds to read this memo – just read the boxed heading for the gist of the holding. The remaining analysis explains the facts, the rationale, and consequences of the decision.

This edition of IPG is accompanied by a podcast featuring Santa Clara County prosecutor Tom Flattery. The podcast will provide **45 minutes of MCLE general credit**. It may be accessed and downloaded for listening at: **http://sccdaipg.podbean.com/**

A Person Has a Reasonable Privacy Expectation Under the Fourth Amendment in Historical Cell Site Location Information (i.e., Records that Can Identify a Person's Past Movements Based on the Person's Cell Phone Usage) Even Though the Information is Captured, Kept, and Controlled by the Cell Phone Carrier. Thus, if the Government Wants to Access Such Information, It Generally Must Obtain a Search Warrant. *Carpenter* v. *United States* (2018) 138 S.Ct. 2206

Facts and Procedural Background

Police officers investigating a series of robberies obtained information from one of the suspected robbers about his accomplices in the robberies. The suspect provided cell phone numbers for some of his accomplices and the FBI "then reviewed his call records to identify additional numbers that he had called around the time of the robberies." (***Id***. at p. 2212.)

Based on that information, the prosecutors applied for court orders under the federal Stored Communications Act to obtain cell phone records for the defendant (one of the suspected robbers.) A federal magistrate judge issued the court order after finding there were "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought were "relevant and material to an ongoing criminal investigation" (i.e., finding the records met the standard for the issuing of such an order). (**Ibid**.)

The order directed the defendant's wireless carriers—MetroPCS and Sprint—to disclose cell site location information (CSLI) for defendant's phone at call origination and at call termination for incoming and outgoing calls during the four-month period when the string of robberies occurred. "The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when defendant's phone was "roaming" in northeastern Ohio. "Altogether the Government obtained 12,898 location points cataloging [the defendant's] movements—an average of 101 data points per day." (**Ibid**.)

Editor's note:** Cell phones function by connecting to a set of radio antennas called "cell sites" located all over the place. "Cell phones continuously scan their environment looking for the best signal [to use for transmission], which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)." (Id***. at pp. 2211-2212.) CSLI can be used to pinpoint a cell phone's user location on a given date and time with increasing precision. (**Ibid**.)

After the defendant was charged with multiple robberies, he moved to suppress the cell-site data provided by the wireless carriers, claiming the seizure of the records "violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause." (**Ibid**.) The motion was denied.

The Sixth Circuit Court of Appeals upheld the trial court's ruling under the rationale that the CSLI was a business record of a wireless carrier and thus, for Fourth Amendment purposes, the defendant "lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers." (***Id***. at p. 2213.)

The High Court took up the case to decide "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." (Id. at p. 2211.)

Holding and Analysis

1. The Fourth Amendment protects individuals against unreasonable searches and seizures. (***Id***. at p. 2213.)

2. Whether government conduct constitutes a "search" was previously "'tied to common-law trespass' and focused on whether the Government 'obtain[ed] information by physically intruding on a constitutionally protected area.'" (**Ibid** [bracketed information added by IPG].)

   However, "property rights are not the sole measure of Fourth Amendment violations." (**Ibid**.) The Fourth Amendment also protects certain expectations of privacy. Thus, as first explained in ***Katz* v. *United States*** (1967) 389 U.S. 347, "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (**Ibid**.)

   Editor's note:** In the dissenting opinion of Justice Thomas, he characterizes the ***Katz test as a "failed experiment" and lays out an interesting case for abandoning it. (***Carpenter*** at pp. 2232-2246.)

3. Currently, "no single rubric definitively resolves which expectations of privacy are entitled to protection," but "the analysis is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted'" and there are "some basic guideposts." (***Id***. at pp. 2213-2214.)

First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." (***Id***. at p. 2214.)

"Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (**Ibid**.)

4. Prior decisions of the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (***id***. at p. 2216, citing to ***Smith* v. *Maryland*** (1979) 442 U.S. 735, 743–744) "even if the information is revealed on the assumption that it will be used only for a limited purpose" (**ibid** citing to ***United States* v. *Miller*** (1976) 425 U.S. 435, 443). "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." (**Ibid**.)

> ***Editor's note:** In ***Smith***, the Court "ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search." In ***Miller***, the Court held the Fourth Amendment did not protect several months of defendant's bank records from a warrantless seizure since the defendant could "assert neither ownership nor possession" of the documents. (***Carpenter*** at p. 2216.)

5. However, the High Court in ***Carpenter*** declined to extend the principle of its earlier decisions in ***Smith*** and ***Miller*** to cell phone location records – given the "unique nature" of those records. The Court observed that "when ***Smith*** was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." (***Carpenter*** at p. 2217.) "There is a world of difference between the limited types of personal information addressed in ***Smith*** and ***Miller*** and the exhaustive chronicle of location information casually collected by wireless carriers today." (***Id***. at p. 2219.)

6. The defendant has some expectation of privacy in his whereabouts. And when the records sought provide the type of "all-encompassing record of the [cell phone] holder's whereabouts" such that the data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'" (***id***. at p. 2217), "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection" (**ibid**).

7. In sum, [w]hether the Government employs its own surveillance technology as in [***United States* v.**] ***Jones*** [(2012) 565 U.S. 400] or leverages the technology of a wireless carrier, . . . an

individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." (***Carpenter*** at p. 2217.) Thus, obtaining the CSLI constitutes a "search" - at least when seeking to access 7 or more days of CSLI. (**Ibid**.)

> ***Editor's note:** In ***Jones***, the Government installed a GPS tracking device on the defendant's automobile. The ***Jones*** court held a "search" of the vehicle had occurred because police "physically occupied private property [of the defendant] for the purpose of obtaining information." (***Id***. at p. 404.) However, a majority of the justices (as evidenced by the two *concurring* opinions in ***Jones***) believed that the *long term monitoring of the vehicle*, tracking every movement a person makes in the vehicle, impinged "on expectations of privacy." (***Carpenter*** at p. 2215 citing to ***Jones*** at p. 430 (opinion of Alito, J.) and ***Jones*** at p. 415 (opinion of Sotomayor, J.). The ***Jones*** court did not decide whether a warrant was required to attach a GPS tracking device to a vehicle – only that it was a search. However, since ***Carpenter*** court found the "search" in the case before it required a warrant (**see** this IPG memo at p. 6), the holding in ***Carpenter*** now strongly suggests that long-term monitoring of a vehicle by attaching a GPS device as in ***Jones*** would also *require a warrant*. (**See** Pen. Code, § 1524(a)(12) [authorizing warrant for use of a tracking device].)

8. The Court declined to address whether the acquisition of CSLI becomes a search only if it extends beyond a limited period: "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." (***Id***. at p. 2217, fn. 3.)

9. The Court rejected the argument that, even assuming a majority of justices on the Court would agree that attaching a GPS device under the circumstances existing in ***United States* v. *Jones*** (2012) 565 U.S. 400 is a search (without any physical trespass), obtaining the CSLI records in the instant case should not be similarly so treated because they only provide the whereabouts of the defendant "within a wedge-shaped sector ranging from one-eighth to four square miles." (***Id***. at p. 2218.)

> ***Editor's note:** The Court appeared to reject this argument - even assuming that this lack of precision might ordinarily be a basis for declining to find a search – based on the concern that *in the future* the CSLI technology would be as precise as the GPS data in ***Jones***. Specifically, the Court stated: "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or ***in development***.' [Citation omitted.] While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision." (***Carpenter*** at pp. 2218–2219, emphasis added by IPG.) This concern for what might happen in the future was echoed in the last portion of the opinion where the Court stated: "[T]he Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." (***Id***. at p. 2223.)

10. The Court also rejected the argument that the user of the cell phone is voluntarily sharing the CSLI in the same way that the bank customer voluntarily shares his or her information with the bank. They did so because: (i) cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society" and (ii) "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up" so that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." (***Id***. at p. 2220.)

11. After finding that the acquisition of the CSLI was a search, the Court concluded that the government "must generally obtain a warrant supported by probable before acquiring the type of CSLI at issue. (***Id***. at pp. 2221.) Thus, an order issued under Section 2703(d) of the Stored Communications Act, which only requires the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation" rather than probable cause, "is not a permissible mechanism for accessing historical cell-site records." (**Ibid**.)

***Editor's note:** Section 2703(d) of the Stored Communications Act, in pertinent part, provides: A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only 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 information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State."

Editor's note:** The Court did not provide much analysis for why probable cause and a warrant would be required other than to point out that "warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." (Id***. at p. 1221.) The Court recognized that the "ultimate measure of the constitutionality of a governmental search is 'reasonableness,'" but then went on to state: "[i]n the absence of a warrant, a search is reasonable ***only*** if it falls within a specific exception to the warrant requirement." (***Id***. at p. 1221, emphasis added by IPG.) The latter language (lifted from some earlier decisions) cannot be reconciled with the statements preceding the language about how "reasonableness" is the ultimate measure of the constitutionality of a search and how warrantless searches are "typically" unreasonable. If the Court means that there must be an already-existing recognized warrant exception to permit the search without a warrant, then the Court could never have approved of warrantless vehicle searches based solely on probable cause or ***Terry*** stops based on reasonable suspicion. If the Court meant that a warrantless search can be justified only if an existing exception applies *or the Court creates a new exception*, then it is devoid of any meaning. Nonetheless, defense counsel will often cite this language in isolation– so prosecutors must be ready to show why it is actually not true and makes no sense. (**See *Cupp* v. *Murphy*** (1973) 412 U.S. 291 [upholding warrantless search not falling into any recognized exception by taking some ingredients from the search incident to arrest, the exigent circumstances, and the ***Terry*** search exceptions (*none of which* individually would justify the search) and mixing them together].)

12. The Court disagreed with one of the dissenting justices (Justice Alito) who contended that the warrant requirement simply does not apply when the Government acquires records using compulsory process such as subpoenas since "subpoenas for documents do not involve the direct taking of evidence [and] they are at most a 'constructive search' conducted by the target of the subpoena." (***Id***. at p. 2221.)

The Court observed that it "has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." (***Ibid***.) "If the choice to proceed by subpoena provided a ***categorical*** limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." (***Id***. at p. 2222, emphasis added by IPG.)

> ***Editor's note:** For a broader discussion of the ramifications of the language of the Court regarding subpoenas for records potentially implicating a suspect's reasonable expectation of privacy, **see** this IPG at pp. 15-18.)

13. The Court qualified the general rule that the government "will generally need a warrant to access CSLI" by pointing out that case-specific exceptions, such as the exigent circumstances exception, may support a warrantless search of an individual's cell-site records. (***Id***. at pp. 2222-2224.)

> ***Editor's note:** For a broader discussion of when the exigency exception will allow warrantless seizure and search of CSLI, **see** this IPG at pp. 8-10.

14. The Court also made sure to highlight the limited scope of its opinion: "Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of ***Smith*** and ***Miller*** or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security." (***Id***. at p. 2223.)

Questions an Inquisitive Prosecutor Might Have After Reading the *Carpenter* Decision

Q-1. Can exigent circumstances justify obtaining either real-time or historical CSLI without a warrant in California?

In ***Carpenter***, the Court recognized that in certain cases, the "the exigencies of the situation" allow for warrantless searches. (***Id***. at p. 2222.) The Court identified such exigencies as including "the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence." (***Id***. at p. 2223.) The Court then went to state, "if law enforcement is confronted with an urgent situation, such fact-specific threats ***will likely justify the warrantless collection of CSLI***. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency." (***Id***. at p. 2223; **see *People* v. *Lively*** (N.Y. App. Div., July 25, 2018) 2018 WL 3566905, *1 [post-***Carpenter*** decision finding no warrant was required to obtain historical CSLI and text messages sent to and received by a cellular phone being used by defendant in hopes of finding a recently missing 17–year–old girl].)

Emergency situations in which CSLI is sought more often than not involve obtaining geolocation data in real-time rather than historical data. (**See *State* v. *Isaac*** (La. Ct. App. 2017) 229 So.3d 1030, 1038 [exigent circumstances existed to track defendant's cell phone where three armed robberies had been committed at various businesses over the span of less than one month, the perpetrators of the crimes were armed with firearms, a an officer testified that it was only a matter of time before a gun accidentally discharged or a victim was shot because he was uncooperative, and police believed defendant was involved in the armed robberies and had information he might become violent towards police and flee the area]; ***People* v. *Valcarcel*** (N.Y. App. Div. 2018) 75 N.Y.S.3d 598, 602 [exigent circumstances existed to track (ping) phone of homicide victim without a warrant]; ***United States* v. *McHenry*** (8th Cir. 2017) 849 F.3d 699, 706 [exigent circumstances existed to track cell phone to prevent juvenile victim from being human trafficked] ***United States* v. *Gilliam*** (2d Cir. 2016) 842 F.3d 801, 802-805 [same]; ***State* v. *Subdiaz-Osorio*** (2014) 357 Wis.2d 41, 46-47 [849 N.W.2d 748, 751] [no warrant

needed to track cell phone location of murder suspect who had fled from Wisconsin and was ultimately tracked to Arkansas where murder occurred less than 24 hours before cell phone data sought]; ***United States* v. *Takai*** (D. Utah 2013) 943 F.Supp.2d 1315, 1323 [exigent circumstance existed for allowing warrantless tracking of cell phone of robbery-shooting suspect]; (**See e.g.**, ***United States* v. *Caraballo*** (D.Vt.2013) 963 F.Supp.2d 341, 362-363 [exigent circumstances existed to track defendant where police had reason to believe that perpetrator of homicide had recently left the scene with the homicide weapon].) But the exigent circumstances exception can exist for both historical and real-time CSLI.

The federal Stored Communications Act (hereinafter "SCA") permits warrantless disclosure by a service provider to a government entity of electronic communication (real-time or historical) "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency . . ." (18 U.S.C.A. § 2702(b)(8); **see also** 18 U.S.C.A. § 2702(c)(4) [allowing disclosure of a "record or other information pertaining to a subscriber to or customer of (cell phone) service" under the same circumstances].) And the California Electronic Communications Privacy Act (hereinafter "CalECPA") allows a government entity to "access electronic device information by means of physical interaction or electronic communication with the device . . . If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information." (Pen. Code, §§ 1546(g); 1546.1(c)(6).) However, assuming section 1546.1(c)(6) even applies to exigent circumstances requests (**see** Flattery's comment on page 9 of this IPG), it only *permits* warrantless "disclosure" of electronic device information; it does not *require* the provider to disclose the information.

The exception for emergencies described in Penal Code section 1546.1(c)(6) would seem to apply to obtaining real-time CSLI because "electronic device information" is defined as: "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." (Pen. Code, §§ 1546(g).) However, expect the defense to argue that the exception in section 1546.1(c)(6) does not permit the disclosure of *historical* CSLI because section 1546.1(c) only applies when the government entity is accessing the device "by means of physical interaction or electronic communication with the device." (Pen. Code, § 1546.1(c).) And when law enforcement seeks historical CSLI they are not *accessing the device* in this manner. Rather, they are seeking to access "electronic communication information" which refers to "any information about an electronic communication or the use of an electronic

communication service, including, but not limited to, . . . location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address." (Pen. Code, § 1546(d).) And there is no statutory exigent circumstances exception for obtaining "electronic communication information" from a service provider. (**See** Pen. Code, § 1546.1(b).)

***Flattery commentary:**

Exigent circumstances requests are governed by the voluntary disclosure section of the SCA. (See 18 U.S.C.A. § 2702(b)(8)&(c)(4).) Under those sections, it is the record holder who must have a good faith belief that there is an exigency. There have been a range of responses from record holders when presented with an exigent request. Some just take the officer's word for it and produce the records. Others ask for details of the investigation and make an independent determination of whether they think there is a sufficient exigency. It is more likely that the latter companies will reject an officer's request.

When CalECPA was initially passed, there was some debate over the scope of the exigent circumstances exception built into section 1546.1(c)(6). Some suggested that CalECPA eliminated the ability of law enforcement to get third-party records in an exigency because the exception only applies when a law enforcement agency is attempting to access a device – and since the agency does not access a third-party record holder's device, there is no authorization. Others argued that a request for disclosure is the functional equivalent of compulsion so that the record holder becomes the agent of the government and thus the law enforcement agency should be treated as directly accessing the device – which would mean that exception for exigent circumstances *would* apply.

In Flattery's opinion, the SCA regulates record holders, not the police; while CalECPA regulates the police, but not record holders. The SCA governs both compelled disclosures and voluntary disclosures. But CalECPA only regulates compelled disclosure and direct access. It does not limit requests for voluntary disclosure. Thus, CalECPA does *not* impact how law enforcement initially obtains voluntary production of CSLI in an exigency. However, once that CSLI is obtained, Penal Code section 1546.1(h) comes into play because it regulates what the government must do after we "obtain" information regardless of whether we obtain that information pursuant to a warrant or under the exigent circumstances exception.

Note: The exigency exceptions defined in CalECPA and the SCA may not be as broad as the exigent circumstance exception to the Fourth Amendment's warrant requirement.

Q-2. Can consent justify obtaining either real-time or historical CSLI without a warrant in California?

One issue left undiscussed in ***Carpenter*** was the question of whether a person who *consents* to the potential distribution of his CSLI data can object to its distribution. "[O]ne of the specifically

established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent." (***Schneckloth* v. *Bustamonte*** (1973) 412 U.S. 218, 219.)

CalECPA does not prevent the government from asking for (as opposed to compelling) electronic communications information from a service provider. (**See** Pen. Code, § 1546.1(a).) CalECPA does prevent the government from "[a]ccess[ing] electronic device information by means of physical interaction or electronic communication with the electronic device. [But] does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity." (Pen. Code, § 1546.1(a)(3).) Moreover, while subdivision (c) of section 1546.1 limits government access to "electronic device information by means of physical interaction or electronic communication with the device" it permits such access "[w]ith the specific consent of the authorized possessor of the device" or "owner of the device, only when the device has been reported as lost or stolen". (Pen. Code, § 1546.1(c)(4)&(5).)

The federal SCA prevents a service provider from disclosing "the contents of a communication while in electronic storage", the "contents of any communication which is carried or maintained on that service", or "a record or other information pertaining to a subscriber to or customer of such service". (18 U.S.C.A. § 2702(a)(1)-(3).) However, a service provider is permitted to divulge the contents of a communication "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." (18 U.S.C.A. § 2702(b)(3).) And the provider may also divulge "a record or other information pertaining to a subscriber to or customer of such service" with "the lawful consent of the customer or subscriber." (18 U.S.C.A. § 2702(c)(2).)

Presumably, there will not be many circumstances in which an officer seeking to track the cell phone belonging to a suspect will seek consent directly from the suspect. However, the suspect may have provided advance consent to release of information to law enforcement, at least under certain circumstances, by way of the contract with the service provider. If nothing else, the terms of the service contract *may* eliminate or reduce the suspect's reasonable expectation of privacy in the CSLI. (*Compare* ***United States* v. *Caraballo*** (D.Vt.2013) 963 F.Supp.2d 341, 362-362 [finding defendant who killed victim and fled had no reasonable expectation of privacy in his cell phone location data because his cell phone company privacy policy informed him that the company may disclose personal information in response to emergencies] *with* ***State* v.**

Subdiaz-Osorio (Wis. 2014) 849 N.W.2d 748, 765 [declining to find Sprint contract stating Sprint will disclose call location if it reasonably believed that an emergency involving immediate danger of death or serious physical injury to any person required disclosure of communications or justified disclosure of records without delay" vitiated defendant's expectation of privacy in CSLI or allowed law enforcement to obtain the information absent a court order].)

***Flattery commentary:** Although advance consent to disclosure by the customer might vitiate the customer's reasonable expectation of privacy for constitutional purposes, under CalECPA, the consent exception *only* applies when the government is seeking direct access to a device. And even then, whether language in a contract allowing disclosure to law enforcement in general would constitute "specific consent" as that term is defined in Penal Code section 1546(k) is questionable. (**See** Pen. Code, § 1546(k) ["Specific consent" means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity."].) In all other instances, consent of the customer is not an exception allowing compelled disclosure of third-party records under CalECPA. Moreover, from a practical standpoint, service providers will not generally give out information based on the theory that the subscriber consented to its disclosure.

Q-3. Should law enforcement get a search warrant to obtain real-time CSLI, historical CSLI involving less than a week of data, or a "tower dump" in California?

In ***Carpenter***, the High Court specifically declined to address the question of whether it was necessary for law enforcement to obtain a warrant before obtaining historical CSLI if law enforcement was requesting less than 7 days-worth of CSLI, real-time CSLI (i.e., the monitoring and tracking of a person based on the person's cell phone pinging cell towers) or "tower dumps" (i.e., a download of information on all the devices that connected to a particular cell site during a particular interval). (***Id***. at p. 2223.)

As the dissenting opinions observed, it will be difficult to draw a logical distinction between historical CSLI data covering more than seven days and real time or historical CSLI covering less than seven days or tower dumps. (See dis. opn. of Kennedy, J. at p. 2234 ["The Court suggests that less than seven days of location may not require a warrant . . . But the Court does not explain why that is so, and nothing in the opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history."]; dis. opn. of Gorsuch, J. at p. 2267 ["what distinguishes historical

data from real-time data, or seven days of a single person's data from a download of everyone 's data over some indefinite period of time? Why isn't a tower dump the paradigmatic example of "too permeating police surveillance" and a dangerous tool of "arbitrary" authority . . .? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?"]; **see also *Tracey* v. *State*** (Fla. 2014) 152 So.3d 504, 520 ["basing the determination as to whether warrantless real time cell site location tracking violates the Fourth Amendment on the length of the time the cell phone is monitored is not a workable analysis"].)

However, regardless of whether the Fourth Amendment requires officers to obtain a warrant for real-time CSLI, CSLI relating to less than 7 days of CSLI, or a tower dump, CalECPA requires a search warrant for such information. (**See** Pen. Code, §§ 1546, 1546.1.) Thus, absent exigent circumstances, law enforcement should always seek a warrant for any real-time CSLI, historical CSLI, or tower dump electronic information.

Q-4. In light of CalECPA, will *Carpenter* require officers in California to change the way they do business when it comes to obtaining CSLI?

Because CalECPA already generally requires a search warrant for CSLI, on a practical level, the decision in ***Carpenter*** should not have much impact on the way officers obtain CSLI in California. However, it might have a slight impact on whether evidence is suppressed.

Before the decision in ***Carpenter***, if officers obtained CSLI from service providers pursuant to the exigent circumstances exception (as defined in CalECPA and the federal SCA) and a court later determined that exigent circumstances did not exist, prosecutors could still argue that no suppression should occur since there was no violation of the *Fourth Amendment* (i.e., because, as all the federal circuits to weigh in on the issue had so concluded, a defendant had no expectation of privacy in that CSLI.) Since CalECPA did not require suppression (it merely *allowed* suppression)* prosecutors were able to make successful arguments that no suppression should occur even if exigent circumstances was belatedly held to be absent. Now that the High Court in ***Carpenter*** has found accessing CSLI without a warrant can be a Fourth Amendment violation, this particular prosecutorial argument will no longer fly.

***Editor's note:**

The plain language of the CalECPA, as well as its statutory history, dictates exclusion *as a remedy for a violation of the statute* is discretionary, and not mandatory. The CalECPA sets forth three remedies to enforce its provisions: "(a) Any person in a trial, hearing, or proceeding ***may move to suppress*** any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5. ¶ (b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter. ¶ (c) An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution." (Pen. Code, § 1546.4 [emphasis added].)

Thus, the plain language of section 1546.4 does not require the exclusion of any evidence seized in violation of the statute. It provides a criminal defendant an avenue to request suppression and implicitly gives the court discretion to impose that remedy. "The plain language of the statute establishes what was intended by the Legislature." (***People* v. *Statum*** (2002) 28 Cal.4th 682, 690.) Accordingly, there is no need to consider the statutory history of the legislation. (***People* v. *Overstreet*** (1986) 42 Cal.3d 891, 895 ["When statutory language is clear and unambiguous, there is no need for construction and courts should not indulge in it."].)

Examining CalECPA's legislative history only reinforces the conclusion reached by examining its plain text alone. This is because the legislature specifically removed language that would have required suppression for statutory violations. In the original version of the bill, section 1564(a) stated: "Except as proof of a violation of this chapter, no evidence obtained or retained in violation of this chapter shall be admissible in a criminal, civil or administrative proceeding, or used in an affidavit in an effort to obtain a search warrant or court order." (See http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_bill_20150209_introduced.htm.) However, this language was deleted from the bill and replaced with the current language. (See http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_bill_20150817_amended_asm_v93.htm.) Had the legislature intended to require suppression it would have kept the original language in the bill or included language similar to that in other statutes requiring exclusion of the evidence obtained in violation of the statute. (See e.g., Evid. Code, § 351.5 ["Notwithstanding any other provision of law, the results of a polygraph examination, the opinion of a polygraph examiner, or any reference to an offer to take, failure to take, or taking of a polygraph examination, shall not be admitted into evidence in any criminal proceeding, including pretrial and post conviction motions and hearings, or in any trial or hearing of a juvenile for a criminal offense, whether heard in juvenile or adult court, unless all parties stipulate to the admission of such results"]; Pen. Code, §§ 631 subd. (c) ["Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding."].) Thus, the drafters of the CalECPA knew how to craft a statute that would mandate exclusion of evidence seized in violation of the statute—and initially contemplated doing so—but specifically chose not to require mandatory exclusion. (**See** Senate Rules Committee Analysis of SB 178 http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_cfa_20150909_094155_sen_floor.html [describing Assembly amendments as "Delet[ing] language in the bill providing that no evidence obtained or retained in violation of the bill's provisions shall be admissible in a criminal, civil, or administrative proceeding, or used in an affidavit in an effort to obtain a search warrant or court order, and add[ing] language providing that parties may move to suppress any electronic information obtained or retained in violation of the law, as specified"].)

Q-5. Can the government *subpoena* CSLI records or other records in which the defendant has a reasonable expectation of privacy?

As noted above in this IPG memo at p. 7, the ***Carpenter*** court rejected the dissenter's claim that because a warrant compelling disclosure of CSLI is akin to subpoenaing documents, the requirement of probable cause and warrant should not be required in order to obtain CSLI. (***Carpenter*** at pp. 2221-2222.)

Dissenting Justice Alito warned that unless the Court's ruling was "somehow restricted to the particular situation in the present case, the Court's move will cause upheaval. Must every grand jury subpoena duces tecum be supported by probable cause? If so, investigations of terrorism, political corruption, white-collar crime, and many other offenses will be stymied. And what about subpoenas and other document-production orders issued by administrative agencies? See, e.g., 15 U.S.C. § 57b–1(c) (Federal Trade Commission); §§ 77s(c), 78u(a)-(b) (Securities and Exchange Commission); 29 U.S.C. § 657(b) (Occupational Safety and Health Administration); 29 C.F.R. § 1601.16(a)(2) (2017) (Equal Employment Opportunity Commission)." (***Carpenter***, dis. opn. of Alito, J. at p. 2247.) "[W]e can guess where today's decision will lead. One possibility is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas duces tecum and all other orders compelling the production of documents will require a demonstration of probable cause, and individuals will be able to claim a protected Fourth Amendment interest in any sensitive personal information about them that is collected and owned by third parties. Those would be revolutionary developments indeed. ¶ The other possibility is that this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered. If we take this latter course, we will inevitably end up 'mak[ing] a crazy quilt of the Fourth Amendment.'" (***Carpenter***, dis. opn. of Alito, J. at pp. 2260-2261.)

Are Justice Alito's concerns valid? Will prosecutors now be faced with defense claims that subpoenas for records in which the defendant has some privacy interest are invalid and prosecutors must use warrants based on probable cause to obtain the records? It is reasonable to expect that some challenges will be made, especially when prosecutors seek records where a colorable argument can be made that the records sought are akin to CSLI in their scope. That being said, most, if not all, such claims should come to naught.

This is because the Court in ***Carpenter*** made efforts to treat CSLI as distinct from other kinds of records: "Justice ALITO overlooks the critical issue. At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." (***Id***. at p. 2222.) Moreover, the Court went on to point out that while the choice to proceed by subpoena did not provide "a categorical limitation on Fourth Amendment protection," it did not mean to say "all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required ***in the rare case*** where the suspect has a legitimate privacy interest in records held by a third party. (***Id***. at p. 2222, emphasis added; **see also *United States* v. *Westley*** (D. Conn., 2018) 2018 WL 3448161, at *14 [finding "Facebook account subscriber information" does not implicate the concerns raised in ***Carpenter*** since the reasoning in ***Carpenter*** was based, in part, on the "unique nature of cell phone location information," which provides "'encyclopedic' information about a person's past movements."].)

Moreover, as observed by Justice Kennedy in his dissenting opinion, subpoenas are often used to obtain private information such as financial records, vehicle registration records, hotel records, employment records and records of utility usage. Yet, *not even* the defendant in ***Carpenter*** questioned this "traditional investigative practice[]." (***Carpenter***, dis. opn. of Kennedy, J. at p. 2229.)

One significant point to make in response to a claim that a search warrant is required to obtain non-CSLI records that allegedly implicate a defendant's reasonable expectation of privacy is that unlike when the government obtained the records in ***Carpenter***, when the government subpoenas records potentially containing material that is privileged or protected by a privacy right, the government cannot receive the records (i.e., breach the defendant's privacy rights) until, inter alia, a court has decided that government has made a sufficient initial showing of good cause for the records (**see *Kling* v. *Superior Court*** (2010) 50 Cal.4th 1068, 1074 [issuance of a subpoena duces tecum does not entitle "the person on whose behalf it is issued to obtain access to the records described therein until a judicial determination has been made that the person is legally entitled to receive them" and "if the third party 'objects to disclosure of the information sought, the party seeking the information must make a plausible justification or a good cause showing of the need therefor.'"]; **accord *People* v. *Blair*** (1979) 25 Cal.3d 640, 651; ***People* v.**

Superior Court (2000) 80 Cal.App.4th 1305, 1316) and that the government interest in obtaining the records outweighs the privacy interests of the persons named in the records (**see *Williams* v. *Superior Court*** (2017) 3 Cal.5th 531, 552 [laying out framework for evaluating whether records potentially protected by the state right of privacy may be released pursuant to a subpoena]; ***People* v. *Webb*** (1993) 6 Cal.4th 494, 516-519 [discussing balancing test used when criminal defendant seeks protected psychiatric records]).

In other words, to the extent a defendant has any expectation of privacy in records (*other than* CSLI) held by a third party that expectation is adequately accommodated by the traditional subpoena process. (**See *Susan S.* v. *Israels*** (1997) 55 Cal.App.4th 1290, 1296 [citing to ***People* v. *Blair*** (1979) 25 Cal.3d 640, 651 for the proposition that "the subpoena duces tecum procedure itself implicitly recognizes an expectation of privacy on the part of the person whose records are subpoenaed."].)

A. What kinds of third-party records are unlikely to be treated the same as CSLI regardless of whether a defendant asserts some privacy interest in the records?

In ***Carpenter***, the majority opinion effectively distinguished, at a minimum, the following kinds of records from CSLI: "Payroll and sales records" citing to ***Donovan* v. *Lone Steer, Inc.,*** (1984) 464 U.S. 408, 411, 415; "Bank Secrecy Act reporting requirements" citing to ***California Bankers Assn. v. Shultz*** (1974) 416 U.S. 21, 67; "financial books and records" citing to ***See v. Seattle*** (1967) 387 U.S. 541, 544; "corporate tax records citing to ***United States* v. *Powell*** (1964) 379 U.S. 48, 49; "books and records of an organization" citing to ***McPhaul* v. *United States*** (1960) 364 U.S. 372, 374, 382; "Federal Trade Commission reporting requirement" citing to ***United States* v. *Morton Salt Co.,*** (1950) 338 U.S. 632, 634, 651–653; "payroll records" citing to ***Oklahoma Press Publishing Co.* v. *Walling*** (1946) 327 U.S. 186, 189, 204–208; and "corporate books and papers" citing to ***Hale* v. *Henkel*** (1906) 201 U.S. 43, 45, 75. (***Carpenter*** at p. 2221, fn. 5.) Records of a similar nature should similarly be treated as distinct from CSLI. (**See e.g., *United States* v. *Westley*** (D. Conn., 2018) 2018 WL 3448161, at *14 [finding "Facebook account subscriber information" does not implicate the concerns raised in ***Carpenter***"].)

One type of record that may be the subject of litigation over whether it is akin to CSLI is the information kept by Google concerning a person's location history. Google has a "location

history" system that uses the phone's location data to build a portrait of where users have traveled with their phones. The history can be viewed in the Timeline tab of Google Maps. Every time the phone establishes a strong enough location point, the system makes an entry in the user's Timeline history, establishing where the user was at that particular time of entry. However, unlike CSLI, a user can disable the location history system and/or clear it for any particular device or for all devices registered with a certain Google account. Moreover, each individual location point can be modified or deleted by the user. (**But see** https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ [claiming Android phones have been collecting the addresses of nearby cellular towers—even when location services are disabled—and sending that data back to Google – but also noting Google is now taking steps to end the practice].) The disabling and editing features may be sufficient to distinguish the Google history information from CSLI, but prosecutors should be prepared to identify other distinguishing aspects as well.

B. Will obtaining a defendant's medical records require a search warrant?

Prosecutors should be prepared to respond to the inevitable defense challenges to prosecutorial subpoenas for a defendant's medical records. California has not really addressed the issue in a published opinion (**but see *People* v. *Finner*** (*unreported*) 2002 WL 1060850, at *1 [finding prosecution could utilize an SDT to a hospital as an independent method from a search warrant to obtain the evidence of a blood draw].) The issue has been flushed out, however, in Texas - at least when it comes to obtaining medical records of a defendant's blood test by way of subpoena. (**See *State* v. *Huse*** (Tex. Crim. App. 2016) 491 S.W.3d 833 ["a DWI offender would have no legitimate expectation of privacy sufficient to block a health care provider from disclosing otherwise protected health care information when required to do so under the terms of a grand jury subpoena"]; ***Rodriguez* v. *State*** (Tex. App. 2015) 469 S.W.3d 626, 636 [**"**HIPAA does not provide Rodriguez with a reasonable expectation of privacy in his medical records and blood-test results in connection with medical treatment for injuries sustained while in custody under suspicion of intoxication."]; ***State* v. *Hardy*** (Tex.Crim.App.1998) 963 S.W.2d 516, 527 [holding there is no Fourth Amendment reasonable expectation of privacy protecting blood-alcohol results from tests taken by hospital personnel solely for medical purposes after a traffic accident]; **cf.**, ***State* v. *Martinez*** (Tex. App. 2017) 534 S.W.3d 97, 101 [review granted] [*seizure and testing of blood sample* drawn by hospital by government required warrant or exigent circumstances].)

Q-6. Must law enforcement obtain a warrant for records which reveal *any* CSLI?

The ***Carpenter*** court specifically declined to "address other business records that might incidentally reveal location information." (***Id***. at p. 2220.) However, it is doubtful that the mere fact that records provide location information about an individual will create the need to obtain a search warrant. This is because the ***Carpenter*** court expressly stated that its decision did not disturb the application of ***Smith*** [**v.** ***Maryland*** (1979) 442 U.S. 735] and [***United States*** **v.**] ***Miller*** [(1976) 425 U.S. 435] or call into question conventional surveillance techniques and tools, such as security cameras." (***Carpenter*** at p. 2220.) And since the records subpoenaed in ***Smith*** and ***Miller*** and information obtained through traditional surveillance tools necessarily reveal location information, it is relatively clear the Court is not going to find the Fourth Amendment to be violated by searches that reveal geolocation data to a lesser extent than the "all-encompassing record of the holder's whereabouts" (***Carpenter*** at p. 2217) embodied in CSLI.

Q-7. Must law enforcement obtain a warrant to conduct other types of surveillance than CSLI?

The holding in ***Carpenter*** should not require law enforcement to obtain a warrant to engage in surveillance that does not otherwise require a warrant. (**Cf.**, Pen. Code, § 1524(a)(12) [authorizing warrant for use of a tracking device in certain circumstances].) As noted above, the Court's holding was not intended to "disturb the application of ***Smith*** and ***Miller or call into question conventional surveillance techniques and tools***, such as security cameras. (***Carpenter*** at p. 2220, emphasis added by IPG.)

Q-8. Will the results of warrantless searches of CSLI that took place before *Carpenter* have to be suppressed?

Prosecutors should anticipate motions being brought by the defense seeking to suppress CSLI data that was obtained without a warrant before ***Carpenter*** issued. Indeed, such motions are already being brought in other jurisdictions. (**See e.g.,** ***United States*** **v.** ***Chavez*** (4th Cir. 2018) 894 F.3d 593, 608; ***United States*** **v.** ***Williams*** (E.D. Mich., 2018) 2018 WL 3659585 and ***United States*** **v.** ***Coles*** (M.D. Pa. 2018) 2018 WL 3659934, at *2, fn. 3; ***United States v. Rojas-Reyes*** (S.D. Ind. 2018) 2018 WL 3439092, at *3; ***United States*** **v.** ***Westley*** (D. Conn. 2018) 2018 WL 3448161, at p. *17.) Because CalECPA already requires a warrant, there should not be too many cases in California where CSLI was obtained without a warrant even before

Carpenter. However, in the event, the defense is challenging the warrantless gathering of CSLI (perhaps from a case not yet final on appeal that pre-dates CalECPA), prosecutors might want to check out the decisions mentioned above – all of which applied the good faith exception to uphold a warrantless seizure of CSLI occurring before the decision in ***Carpenter***.

The reasoning of these cases is similar, and they generally reach their conclusions while acknowledging that the rule in ***Carpenter*** is a new rule and that it should be applied retroactively in accordance with ***Griffith* v. *Kentucky*** (1987) 479 U.S. 314 – a case holding new rules announced by the Supreme Court apply retroactively to all cases on direct review or not yet final. The Fourth Circuit in ***United States* v. *Chavez*** (4th Cir. 2018) 894 F.3d 593 provided a good summary of the reasoning:

"The exclusionary rule's 'sole purpose ... is to deter future Fourth Amendment violations." ***Davis* v. *United States***, 564 U.S. 229, 236–37 (2011). Thus, when investigators "act with an objectively 'reasonable good-faith belief' that their conduct is lawful," the exclusionary rule will not apply. ***Id***. at 238 (quoting ***United States* v. *Leon***, 468 U.S. 897, 909 (1984)). Objectively reasonable good faith includes 'searches conducted in reasonable reliance on subsequently invalidated statutes.' ***Id***. at 239. [The defendant] does not, and cannot, deny that investigators in this case reasonably relied on court orders and the Stored Communications Act in obtaining the cell site records. Without question, then, the good-faith exception to the exclusionary rule applies to investigators' actions here." (***Chavez*** at p. 608 [alternate citations omitted throughout]; **see also *People* v. *Willis*** (2002) 28 Cal.4th 22, 30 [noting the prime purpose of the exclusionary rule is to deter "future unlawful police misconduct" and "its application is restricted to those situations in which its remedial purpose is effectively advanced'"]; ***United States* v. *Brown*** (C.D. Cal. 2017) 2017 WL 3428300, at *4 [pre-***Carpenter*** case acknowledging that "[n]either the Ninth Circuit nor the Supreme Court has yet adjudicated the question of whether the warrantless seizure and search of CSLI violates the Fourth Amendment" but that "[g]iven the still evolving state of the law and the Supreme Court's forthcoming resolution of this question," concluding "that—even if the Fourth Amendment protects the historical CSLI at issue in this case—the evidence is admissible under the good faith exception to the exclusionary rule."]; ***United States* v. *Gray*** (D. Ariz. 2017) 2017 WL 3675383, at pp. *5-*6 [pre-***Carpenter*** case reaching same conclusion as ***Brown*** and contrasting the "small minority of district court cases that have found collection of CSLI subject to a probable cause requirement" with the overwhelming federal case law to the contrary].)

Even if law enforcement did not use a SCA section 2703(d) order, and instead relied on the exigent circumstances exception in 18 U.S.C. § 2702(c)(4) of the SCA, to obtain CSLI without a warrant, the good faith exception should apply to prevent exclusion of the evidence. (**See *State* v. *Malveaux*** (La. Ct. App. 2018) 245 So.3d 81, 90-92.)

NEXT EDITION OF IPG: WHAT ARE THE RULES REGARDING CONTACTING AND EXTRACTING INFORMATION FROM DEFENSE EXPERTS?

Suggestions for future topics to be covered by the Inquisitive Prosecutor's Guide, as well as any other comments or criticisms, should be directed to Jeff Rubin at (408) 792-1065.