LEGISLATIVE COUNSEL BUREAU
925 L STREET
SACRAMENTO, CALIFORNIA 95814
TELEPHONE (916) 341-8000
FACSIMILE (916) 341-8020
INTERNET WWW.LEGISLATIVECOUNSEL.CA.GOV

August 1, 2019

Honorable Jacqui Irwin
Room 5119, State Capitol

CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT - #1916004

Dear Ms. Irwin:

California's Electronic Communications Privacy Act (Pen. Code, § 1546 et seq.)[1] (hereafter CalECPA) generally restricts government access to electronic information without a warrant or wiretap order, with certain exceptions. In some circumstances, the CalECPA allows a government entity to take specified actions involving electronic information if it obtains specific consent to do so. You have asked whether the CalECPA restricts a department of a city or county from requiring a business that rents dockless bikes, scooters, or other shared mobility devices to the public (hereafter dockless mobility provider) to provide the department with real-time location data from its dockless shared mobility devices (hereafter real-time data-sharing requirement) as a condition of granting a permit to operate in the department's jurisdiction. You have also asked whether, in order to constitute specific consent for purposes of the CalECPA, it is necessary for an individual to provide consent directly to a government entity seeking that individual's data.

Background: CalECPA

The CalECPA restricts government access to electronic information by prohibiting a government entity from (1) "Compel[ling] the production of or access to electronic communication information from a service provider," (2) "Compel[ling] the production of or access to electronic device information from any person or entity other than the authorized possessor of the device," or (3) "Access[ing] electronic device information by means of physical interaction or electronic communication with the electronic device" without a warrant or wiretap order, with certain exceptions. (§ 1546.1, subd. (a).)

As relevant to the issues presented, and as an exception to the third prohibition enumerated above, the CalECPA allows a government entity to access electronic device

[1] All further section references are to the Penal Code unless otherwise provided.

information by means of physical interaction or electronic communication with the device with the specific consent, as defined, of the authorized possessor of the device. (§ 1546.1, subd. (c)(4).) However, this authorization does not extend to actions to compel electronic information from a service provider or person or entity other than an authorized possessor. (See § 1546.1, subd. (b).)

1. Does the CalECPA restrict a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider as a condition of granting a permit to operate in the department's jurisdiction?

1.1 Analysis

1.1.1 Whether a department of a city or county is a government entity for the purposes of the CalECPA

As an initial matter, we must determine whether a department of a city or county is a government entity for the purposes of the CalECPA. "Government entity" is defined for these purposes as "a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf the state or a political subdivision thereof." (§ 1546, subd. (i).)

Counties are political subdivisions of the state under both state and federal law. (*County of Inyo v. City of Los Angeles* (1978) 78 Cal.App.3d 82, 90; *U.S. v. Nez Perce County, Idaho* (9th Cir. 1938) 95 F.2d 238.) Accordingly, a department of a county is a department of a political subdivision of the state and therefore a government entity for the purposes of the CalECPA.

Cities are political subdivisions of the state under federal law (*City of Ontario, Cal. v. Quon* (2010) 560 U.S. 746, 750; *City of Trenton v. State of New Jersey* (1923) 262 U.S. 182, 185-186), but have generally not been considered political subdivisions of the state under state law (*Blum v. City and County of San Francisco* (1962) 200 Cal.App.2d 639, 643). Accordingly, the phrase "the state or a political subdivision thereof," as used in the CalECPA, is reasonably susceptible to two interpretations, one of which includes a city, and the other of which does not.

To resolve this ambiguity, we turn to the legislative history of the CalECPA. (See *People v. Cornett* (2012) 53 Cal.4th 1261, 1265.) Here, two aspects of the legislative history of the CalECPA suggest that its definition of "government entity" was informed by federal law, not state law.

The first aspect is the CalECPA's relationship to the federal Electronic Communications Privacy Act of 1986 (Pub.L. No. 99-508, 100 Stat. 1848) (hereafter federal ECPA or federal act). That federal act, like the CalECPA,[2] was passed to protect the privacy interests of private citizens against government intrusion. (See *Suzlon Energy Ltd. v. Microsoft*

[2] See Assem. Com. on Privacy & Consumer Protection, Analysis of Sen. Bill No. 178 (2015-2016 Reg. Sess.) as amended June 2, 2015, pp. 5-6.

Corp. (9th Cir. 2011) 671 F.3d 726, 730.) The CalECPA's name indicates that the Legislature considered the federal act when adopting the state act,[3] and various definitions used in the CalECPA appear to be derived from the federal ECPA. (Compare § 1546, subd. (c), with 18 U.S.C. § 2510(12); compare § 1546, subd. (e) with 18 U.S.C. § 2510(15).) Accordingly, we think that a court would view the federal ECPA's definition of "governmental entity" as helpful to an understanding of the subsequent CalECPA definition of the term "government entity." (See *Friends of Mammoth v. Board of Supervisors* (1972) 8 Cal.3d 247, 260.) That federal act defines "governmental entity" as "a department or agency of the United States or any State or political subdivision thereof." (18 U.S.C. § 2711(4).) Cities are included in this federal definition as "political subdivisions" of the state under federal law. (See *City of Trenton v. State of New Jersey, supra,* 262 U.S. at pp. 185-186). In our view, therefore, a court would construe the CalECPA's definition of "government entity" consistently with that federal definition to also include cities and city departments.

The second aspect is the legislative motivation behind the CalECPA. Committee analyses of Senate Bill No. 178 of the 2015-2016 Regular Session (Stats. 2015, ch. 651) (hereafter SB 178), the bill that enacted the CalECPA, indicate that the CalECPA was motivated by a perception that both federal and state protections against government access to electronic information, including those provided by the federal ECPA, were inadequate.[4] A broader interpretation of the government entities subject to the CalECPA would provide greater protection against government access to electronic information and therefore comport more closely with the legislative motivation for the CalECPA than a narrow interpretation of the term.

Consequently, although a reasonable argument may be made to the contrary, it is our view that a department of a city is a government entity for the purposes of the CalECPA.

---

[3] Committee analyses of the bill that enacted the CalECPA also discuss the federal ECPA as constituting part of the legal background for the CalECPA. (See Sen. Com. on Appropriations, Analysis of Sen. Bill No. 178 (2015-2016 Reg. Sess.) as amended Apr. 22, 2015, p. 2; Assem. Com. on Privacy & Consumer Protection, Analysis of Sen. Bill No. 178 (2015-2016 Reg. Sess.) as amended June 2, 2015, p. 6; see also Assem. Com. on Public Safety, Analysis of Sen. Bill No. 178 (2015-2016 Reg. Sess.) as amended July 7, 2015, p. 10.)

[4] See, e.g., Assem. Com. on Privacy & Consumer Protection, Analysis of SB 178, as amended June 2, 2015, p. 6 ("Unfortunately, technology continued to advance rapidly since the [federal ECPA's] inception nearly 30 years ago and amendments to the Act have not always kept pace. [¶] The author contends that the federal statute 'has not been meaningfully updated to account for modern technology,' ... [¶] [and] also cites a variety of situations where California law already explicitly requires a warrant for many kinds of information ... . [¶] As a result, the author and supporters believe that existing law is insufficient to protect all forms of electronic communications and their meta-data ...").

1.1.2 The CalECPA's prohibition on compelling the production of or access to electronic communication information from a service provider

The CalECPA's first general prohibition restricts a government entity from "Compel[ling] the production of or access to electronic communication information from a *service provider*." (§ 1546.1, subd. (a)(1); emphasis added.) Thus, unless a dockless mobility provider is a service provider, this prohibition would not restrict a department of a city or county from imposing a real-time data-sharing requirement on that dockless mobility provider.

In this regard, "service provider" is defined for the purposes of the CalECPA as "a person or entity offering an electronic communication service." (§ 1546, subd. (j).) "Electronic communication service," in turn, is defined as "a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information." (§ 1546, subd. (e).)

It is our understanding that, unlike internet service providers or providers of email or bulletin board systems, dockless mobility providers do not offer to provide users with the ability to send or receive electronic communications or act as intermediaries in the transmission of electronic communications.[5] Similarly, dockless mobility providers do not offer to store electronic communication information for others. Accordingly, it is our view that a dockless mobility provider is not "a person or entity offering an electronic communication service." (§ 1546, subd. (j).)

Consequently, we conclude that a dockless mobility provider is not a service provider within the meaning of the CalECPA and that the CalECPA's first general prohibition would therefore not restrict a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider as a condition of granting a permit.

1.1.3 The CalECPA's prohibition on compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device

The CalECPA's second general prohibition restricts a government entity from "*Compel[ling]* the production of or access to *electronic device information* from any person or entity other than the *authorized possessor* of the device." (§ 1546.1, subd. (a)(2); emphasis

---

[5] See *In re Google Inc. Cookie Placement Consumer Privacy Litigation* (3d Cir. 2015) 806 F.3d 125, 146 (observing that the phrase "'any service which provides to users thereof the ability to send or receive wire or electronic communications' most naturally describes network service providers"); *Facebook, Inc. v. Superior Court* (2018) 4 Cal.5th 1245, 1268; *U.S. v. Warshak* (6th Cir. 2010) 631 F.3d 266, 286 (describing internet service providers as the "intermediar[ies] that make[] email communication possible").

added.) Thus, in order for this prohibition to restrict a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider, all three of the following elements must apply: (1) real-time location data from dockless shared mobility devices must be electronic device information, (2) a dockless mobility provider must be a person or entity other than the authorized possessor of the device, and (3) the imposition of a permitting requirement must constitute "compel[ling] the production of or access to" that information.

With regard to the first element, "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.*" (§ 1546, subd. (g); emphasis added.) "Electronic device," in turn, is defined as "a device that stores, generates, or transmits information in electronic form," excluding the magnetic strip on a state driver's license or identification card. (§ 1546, subd. (f).) It is our understanding that all dockless shared mobility devices, as part of their dockless functionality, necessarily store and transmit location data and other information in electronic form.[6] Consequently, it is our view that the first element described above would be satisfied because a dockless shared mobility device is an "electronic device" and information regarding the current and prior locations of a dockless shared mobility device is therefore electronic device information for the purposes of the CalECPA.

With regard to the second element, "authorized possessor" is defined as "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device." (§ 1546, subd. (b).) Thus, a person is an authorized possessor of an electronic device if that person owns and possesses the device or possesses the device under authorization from the device's owner to do so. Although a dockless mobility provider presumably owns the dockless shared mobility devices that it offers for rent, it also authorizes each user to possess a device for the duration of the user's rental and therefore does not possess the device during the period of that rental. Thus, it is our view that the second element described above is satisfied because, to the extent that a real-time data-sharing requirement would require the sharing of real-time location data from a dockless shared mobility device while that device is being rented, that requirement would require obtaining data from a person or entity other than the authorized possessor of the device.

---

[6] See Thomson Reuters, Practical Law Gov. Practice Note No. W-017-6569, Dockless Mobility Regulation (2018) ("Dockless bikes or scooters allow riders to rent a bicycle or scooter by using an app that will let the user know where an available bike is located. After finding the nearest bike, users scan a code on their phone, then the bike unlocks and is available for use"); Baumgaertner, *Bike-Sharing Is Flourishing in Washington. Can the City Handle It?*, N.Y. Times (Oct. 1, 2017), available at <https://www.nytimes.com/2017/10/01/us/politics/washington-bike-share.html> (as of July 16, 2019) (describing dockless shared bikes as GPS-tracked and electronically locked).

With regard to the third element, unlike the terms "electronic device information" and "authorized possessor," the term "compel" is not statutorily defined for the purposes of the CalECPA. Further, although a court may refer to dictionary definitions of a term in order to discern its meaning (*Smith v. Selma Community Hospital* (2010) 188 Cal.App.4th 1, 30, as mod. on denial of rehg. Sept. 27, 2010), the dictionary definition of "compel" as "to drive or urge forcefully or irresistibly" or "to cause to do or occur by overwhelming pressure" (Webster's Online Dict., definition of "compel," at <https://www.merriam-webster.com/dictionary/compel> [as of July 18, 2019]) does not clearly include or exclude permitting requirements. Accordingly, we turn to the legislative history of the CalECPA for guidance. (See *People v. Cornett, supra,* 53 Cal.4th at p. 1265.)

Here, that legislative history indicates that the CalECPA was intended to codify and expand privacy protections under Fourth Amendment jurisprudence and existing state and federal statutes. (Sen. Rules Com., Off. of Sen. Floor Analyses, 3d reading analysis of SB 178, as amended Sept. 4, 2015, pp. 3-4.) The Legislature passed that act in the wake of two major United States Supreme Court cases on search and seizure rights under the Fourth Amendment to the United States Constitution, *U.S. v. Jones* (2012) 565 U.S. 400 and *Riley v. United States* (2014) 573 U.S. 373, and intended that the act strengthen existing privacy protections by creating a "clear, uniform warrant rule for California law enforcement access to electronic information." (Assem. Com. on Privacy & Consumer Protection, Analysis of SB 178, as amended June 2, 2015, p. 7.)

In order to be consistent with this legislative intent to codify and expand privacy protections under Fourth Amendment case law and to impose a "uniform warrant rule," the scope of government actions encompassed by the term "compel" for the purposes of the CalECPA must be at least as broad as the range of government actions that are restricted under the Fourth Amendment. The CalECPA imposes conditions on warrants for electronic information that are more stringent than those required by the Fourth Amendment.[7] Thus, a narrow construction of the term "compel" that would subject some government attempts to procure electronic information to the more stringent CalECPA warrant requirements but subject other attempts to existing Fourth Amendment requirements would be inconsistent with the Legislature's intent that the CalECPA impose a "clear, uniform warrant rule."

A construction of the term "compel" that is narrower than the range of government actions that are restricted under the Fourth Amendment would also be inconsistent with the Legislature's intent to codify and expand Fourth Amendment case law.

---

[7] Compare § 1546.1, subd. (d)(2) (a warrant for electronic information must require that all unrelated information obtained through the execution of the warrant shall be sealed and not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery) with *U.S. v. Adjani* (9th Cir. 2006) 452 F.3d 1140, 1151 ("There is no rule ... that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evidence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant").

Under Fourth Amendment case law, a government entity may not, absent consent, exigent circumstances, or certain other limited circumstances, conduct an administrative search of a business's private facilities or records for regulatory purposes without a warrant or administrative subpoena. (*City of Los Angeles v. Patel* (2015) 576 U.S. __ [135 S.Ct. 2443, 2452-2453] (hereafter *Patel*).) In *Patel,* the United States Supreme Court held that a provision of the Los Angeles Municipal Code that required a hotel to give its guest registry to the police for inspection without any warrant, administrative subpoena, or the opportunity for precompliance review, and imposed criminal penalties for noncompliance was facially unconstitutional under the Fourth Amendment. (*Id.* at p. 2456.) In *De La Cruz v. Quackenbush* (2000) 80 Cal.App.4th 775 (hereafter *De La Cruz*), a California Court of Appeal similarly struck down a warrantless regulatory inspection scheme for insurance brokers and held that the Insurance Commissioner exceeded his authority in revoking a broker's brokerage license for refusing to surrender documents in response to an insurance department investigator's warrantless and subpoena-less demand for those documents.

We find no relevant distinction between a permitting system that imposes a real-time data-sharing requirement and the municipal ordinance invalidated in *Patel* or the regulatory inspection scheme struck down in *De La Cruz*. The department, like the police officers in *Patel* and the investigator in *De La Cruz*, would be requiring the production of protected information without a warrant, administrative subpoena, or opportunity for precompliance review, and the regulated person or entity would suffer consequences as a result of the failure to produce the required information. Accordingly, it is our view that the imposition of such a permitting requirement would constitute the "[c]ompel[ling of] the production of or access to" electronic device information under the CalECPA.

Consequently, we conclude that the CalECPA's second general prohibition restricts a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider as a condition of granting a permit.

1.1.4 The CalECPA's prohibition on accessing electronic device information by means of physical interaction or electronic communication with the electronic device

The CalECPA's third general prohibition restricts a government entity from "Access[ing] electronic device information by means of physical interaction or electronic communication with the electronic device." (§ 1546.1, subd. (a)(3).) Unlike the first two general prohibitions, which restrict a government entity from procuring electronic information from third parties (§ 1546.1, subd. (a)(1) & (2)), this prohibition restricts a government entity from procuring that information from an electronic device itself. Thus, the text and context of the third general prohibition suggest that the prohibition was intended to address situations where a government entity is able to procure electronic data without the consent or assistance of a third party.

This interpretation of that prohibition is consistent with the legislative history of the CalECPA. Committee analyses of SB 178 provide that the CalECPA was enacted, in part, to address privacy concerns raised by United States Supreme Court cases in which law enforcement procured electronic information directly from electronic devices by scrolling

through contacts on a cell phone or installing and collecting data from a GPS tracking device, or other instances in which a government agency acquires electronic information without a physical intrusion, such as when it wirelessly extracts data from cellphones and other cellular data devices by using a separate device capable of mimicking a wireless carrier cell tower. (Assem. Com. on Public Safety, Analysis of SB 178, as amended July 7, 2015, pp. 8-9, discussing *Riley v. United States* (2014) 573 U.S. 373 & *U.S. v. Jones* (2012) 565 U.S. 400.) All of these scenarios involve instances in which a government entity has the practical capability of procuring electronic data without the consent or assistance of another person or entity and therefore would not be practically precluded from obtaining that data by either of the CalECPA's first two general prohibitions.

Accordingly, it is our view that the CalECPA's third general prohibition restricts a government entity from itself directly procuring electronic device information from an electronic device and does not extend to situations in which a government entity seeks to procure that information, or a means to procure that information, from a third party. Because the imposition of a real-time data-sharing requirement on a dockless mobility provider would involve the procurement of electronic information, or a means to procure that information, from a third party and not the dockless shared mobility devices themselves, it is our view that the CalECPA's third general prohibition would not restrict a government entity from imposing that requirement.

Thus, we conclude that the CalECPA's third general prohibition does not restrict a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider prohibition. However, as discussed above, because the CalECPA restricts a government entity from "Compel[ling] the production of or access to electronic device information from any person or entity other than the authorized possessor of the device" (§ 1546.1, subd. (a)(2)), that act would restrict a department of a city or county from imposing a real-time data-sharing requirement on a dockless mobility provider as a condition of granting a permit.

1.2 Conclusion regarding Question No. 1

It is our opinion that the CalECPA restricts a department of a city or county from requiring a business that rents dockless bikes, scooters, or other shared mobility devices to the public to provide the department with real-time location data from its dockless shared mobility devices as a condition of granting a permit to operate in the department's jurisdiction.

2. In order to constitute "specific consent" for purposes of the CalECPA, is it necessary for an individual or entity to provide consent directly to the government entity seeking that individual's data?

2.1 Analysis

As discussed above, the CalECPA prohibits a government entity from "Access[ing] electronic device information by means of physical interaction or electronic communication with the electronic device" without a warrant or wiretap order, with certain

exceptions. (§ 1546.1, subd. (a)(3).) As an exception to that prohibition, the CalECPA allows a government entity to access electronic device information under those circumstances with the specific consent of the authorized possessor of the device (§ 1546.1, subd. (c)(4)) or, when the device has been reported as lost or stolen, with the specific consent of the owner of the device (*id.*, subd. (c)(5)). In addition, a government entity must destroy information voluntarily provided by a service provider within 90 days unless an exception applies, including that the government entity "obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed." (*Id.*, subd. (g)(1).) The definition of "specific consent" for these purposes is set forth in section 1546, subdivision (k), which reads:

> "'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." (Emphasis added.)

When statutory language is clear and unambiguous, courts will not speculate that the Legislature meant something other than what it said. (*Martin Brothers Construction, Inc. v. Thompson Pacific Const., Inc.* (2009) 179 Cal.App.4th 1401, 1411.) Here, section 1546, subdivision (k) explicitly provides that "specific consent," for the purposes of the CalECPA, means "consent provided directly to the government entity seeking information." Accordingly, we conclude that an individual must provide consent directly to the government entity seeking that individual's data in order to constitute "specific consent" within the meaning of the CalECPA.

2.2 Conclusion regarding Question No. 2

It is our opinion that, in order to constitute "specific consent" for purposes of the CalECPA, it is necessary for an individual or entity to provide consent directly to the government entity seeking that individual's data.

Very truly yours,

Diane F. Boyer-Vine
Legislative Counsel

By
Mariko M. Kotani
Deputy Legislative Counsel

MMK:kam