



August 23, 2019

The Honorable Toni Atkins
Senate President Pro Tempore
State Capitol Building
Room 205
Sacramento, CA 95814

The Honorable Anthony Rendon
Speaker of House
Capitol Office, Room 219
Sacramento, CA 94249

Re: Legislation is Needed to Set Clear Limits on Local Authorities' Access to Individual Trip Data

Dear Mr. Rendon and Ms. Atkins:

I write on behalf of the Electronic Frontier Foundation (EFF) to highlight the need for legislation protecting *individual trip data*—data pertaining to individual trips or rides taken via transportation network companies (TNCs), shared mobility devices (such as scooters, electronic bicycles, or on-demand shared vehicles), or other new forms of transportation. EFF is a San Francisco-based non-profit organization that works to protect privacy and civil liberties in the digital age. EFF represents approximately 40,000 active donors and members, including thousands of supporters in California.

Local and regional planning agencies in jurisdictions across the United States are increasingly demanding access to data about new mobility services and devices in order to better plan for the future and ensure that city streets work for everyone. EFF agrees that planning agencies should be able to collect some data in order to ensure that new transportation devices are deployed safely, efficiently, equitably, and sustainably. But planning agencies should not need to collect sensitive, personally identifiable information about riders in order to do so.

Individual trip data is sensitive location data that pertains to movements of real individuals, and it should be off-limits for city or regional planning purposes. Instead, local authorities can and should be using aggregated and deidentified trip data to achieve their planning goals without sacrificing the privacy of Californians.

Unfortunately, not all local authorities have shown a willingness to balance their planning goals with the privacy interests of their residents, even when doing so violates the California Constitution and the California Electronic Communications Privacy Act (CalECPA). Clear limits from the Legislature are needed to protect the privacy of

Californians and rein in efforts by local authorities to obtain access to sensitive individual trip data.

I. Individual Trip Information is Sensitive Data that Pertains to the Movements of Real Individuals.

Individual trip data typically includes time-stamped start and end points as well as granular route information. This data can be deeply revealing. As the United States Supreme Court recognized in *Carpenter v. United States*, time-stamped location 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.’”¹ As the Court explained, “location records hold for many Americans the privacies of life.”² For example, time-stamped geolocation data can reveal trips to Planned Parenthood, specific places of prayer, and gay-friendly neighborhoods or bars. Patterns in the data can reveal social relationships, and potentially even extramarital affairs, as well as personal habits, such as when people typically leave for work, go to the gym, or run errands, how often they go out on evenings and weekends, and where they like to go.

Even with names stripped out, location information is notoriously easy to re-identify,³ particularly for habitual trips. This is especially true when location information is aggregated over time. As one 2013 study on human mobility data concluded, “human mobility traces are highly unique.”⁴ Researchers found that only “four spatio-temporal points [were] enough to uniquely identify 95% of the [1.5 million] individuals” in the study.⁵

In another example, when a data scientist released a database of every cab ride taken in New York City in 2013—containing records on 173 million trips, including pickup and drop-off locations and times, as well as putatively anonymized hack license numbers and medallion numbers and other metadata—one researcher was able to de-anonymize the

¹ *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

² *Id.* at 2217 (2018) (internal quotations and citations omitted).

³ See CDT, Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility (Nov. 29, 2018), <https://cdt.org/insight/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/>.

⁴ See Yves-Alexandre de Montjoye et al., Unique in the Crowd: The privacy bounds of human mobility, *Scientific Reports* 3, Article Number 1376 (Mar. 23, 2013), available at <http://www.nature.com/articles/srep01376>.

⁵ See *id.* The study relied on 15 months of human mobility data for 1.5 million individuals, where the location of each individual had been specified hourly.

entire set (thus re-identifying the hack license numbers and medallion numbers for each trip) with relative ease.⁶ Another researcher then used the data—in combination with other readily available data tying particular individuals to particular locations—to identify individual riders, where they went, and their personal habits or routines.⁷

As the California Legislature determined last year in enacting the California Consumer Privacy Act (CCPA), any information that can be reasonably linked, *directly or indirectly*, with a particular consumer should be considered “personal information.”⁸ The Legislature explicitly listed geolocation information as one such category of information.⁹

Given the sensitive nature of individual trip data, this data should be off-limits for city or regional planning purposes. Local authorities and planning agencies should be required to use aggregated and deidentified trip data—such as data relating to groups of trips taken within an hour between census blocks. Aggregated and deidentified data can provide important insights into how Californians are using TNCs and shared mobility devices for their transportation needs. Limiting local authorities to such data strikes the appropriate balance between protecting individual privacy and ensures that local authorities have the information they need to regulate our public streets so that they work for all Californians.

Importantly, limiting local authorities to aggregated and deidentified *trip data* will not restrict access to data regarding individual mobility devices when those devices are not “on trip,” and thus not tied to the movements of any particular individual. A limitation on the use of individual trip data, for example, will not get in the way of cities’ efforts to monitor and enforce equitable distribution requirements for scooters or electronic bikes.

⁶ The researchers were able to re-identify the hack license number and medallion numbers, because New York had used an insufficient hashing algorithm to anonymize the data. Vijay Pandurangan, On Taxis and Rainbows, Lessons from NYC’s improperly anonymized taxi logs, Medium (June 21, 2014), <https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1>.

⁷ Anthony Tockar, Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset (Sep. 15, 2014), <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/>; see also J.K. Trotter, Public NYC Taxicab Database Lets You See How Celebrities Tip, *Gawker* (Oct. 24, 2014), <https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546>.

⁸ See Cal. Civ. Code § 1798.140(o)(1) (“‘Personal information’ means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: . . . (G) Geolocation data.”) (effective Jan. 1, 2020).

⁹ *Id.*

II. Efforts to Collect Data First—and Think About What to Do With it Later—Violate the Letter and Spirit of the California Constitution.

When it comes to the data privacy, the biggest mistake local jurisdictions could make would be to collect data first and think about what to do with it later—after consumers’ privacy has been put at risk. That, however, is what is currently happening in jurisdictions across the United States, including in California.

In California, these efforts violate the right to privacy afforded by Article I, Section 1 of the California Constitution, which explicitly lists privacy as an inalienable right of all people.¹⁰ As the California Supreme Court has recognized, “[i]nformational privacy is the core value furthered by” the explicit inclusion of the right to privacy in the state constitution.¹¹ The Court has further explained that “the moving force” behind California’s constitutional right to privacy was concern over “the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society[.]”¹² Inclusion of the right to privacy recognizes that “[t]he proliferation of government . . . records over which we have no control limits our ability to control our personal lives.”¹³ And pursuant to the right to privacy, any incursion into individual privacy “must be justified by a compelling interest.”¹⁴

The right of privacy not only “prevents government and business interests from collecting and stockpiling unnecessary information about us[.]” but also “*from misusing information gathered for one purpose in order to serve other purposes[.]*”¹⁵ Indeed, such

¹⁰ Cal. Const., art. I, § 1 (“All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy.*”) (emphasis added); *see also* Civ. Code § 1798.1 (“The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them.”).

¹¹ *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35 (1994); *see also Los Angeles Gay & Lesbian Ctr. v. Superior Court*, 194 Cal. App. 4th 288, 307 (2011) (citation and internal quotations omitted) (“[T]he privacy right protects the individual’s reasonable expectation of privacy against a serious invasion.”).

¹² *White v. Davis*, 13 Cal. 3d 757, 774 (1975).

¹³ *Id.* at 775.

¹⁴ *White*, 13 Cal. 3d at 775.

¹⁵ *Hill*, 7 Cal. 4th at 17 (citation omitted, emphasis added).

“improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party[]” is among the “principal ‘mischiefs’” targeted by the right.¹⁶

Legislation limiting local authorities to aggregated and deidentified trip data will help ensure compliance with the letter and spirit of Article I, Section 1 of the California Constitution.

III. Efforts to Require Individual Trip Data as a Condition of Receiving a Permit to Operate Shared Mobility Devices Violate CalECPA.

Multiple California cities are also currently operating programs related to shared mobility devices that are in blatant violation of CalECPA. These programs require that providers of shared mobility devices, as a condition of receiving a permit to operate, turn over data relating to individual trips.

CalECPA, however, provides that “a *government entity* shall not . . . [c]ompel the production of or access to *electronic device information* from any person or entity other than the authorized possessor of the device” except in specific circumstances—such as when the government entity has a warrant or a wiretap order or, in cases where the information is not sought in connection with a criminal offense, a subpoena issued pursuant to existing state law, so long as access to the information via a subpoena is not otherwise prohibited by law.¹⁷

First, as is clear from the plain language of the statute, this provision is *not limited to law enforcement*. On its face, it applies to any government entity, defined to include any “department or agency of the state or a political subdivision thereof[.]”¹⁸

Second, this provision of CalECPA covers both (a) electronic bikes and scooters—which are “electronic devices,” *i.e.*, “device[s] that store[], generate[], or transmit[] information in electronic form”¹⁹—and (b) the geolocation information they generate—which

¹⁶ *White*, 13 Cal. 3d at 775.

¹⁷ Cal. Pen. Code § 1546.1(a), (b) (emphasis added).

¹⁸ Cal. Pen. Code § 1546(i).

¹⁹ Cal. Pen. Code § 1546(f).

constitutes both “electronic device information”²⁰ or “electronic information”²¹ under the statute. CalECPA thus applies when any government agency—including a city transportation planning agency—attempts to obtain raw, individual trip data about a shared bike or scooter from anyone other than the rider (*i.e.*, the authorized possessor).²²

On August 1, 2019, the California Legislative Counsel issued an opinion letter confirming the CalECPA applies to geolocation data pertaining to shared mobility devices. (Attached hereto as Attachment A). The letter—issued in response to an inquiry from Assemblywoman Jacqui Irwin regarding whether CalECPA restricts a city or county department from requiring a business that rents shared mobility devices to the public to provide access to real-time location data as a condition of obtaining an operating permit—makes four key findings:

- First, both cities and counties constitute political subdivisions of the state for purposes of CalECPA and are thus “government entities” covered by statute.²³
- Second, “information regarding the current and prior locations of a dockless shared mobility device” is electronic device information.²⁴
- Third, dockless mobility providers are persons or entities other than the authorized possessors of the devices (*i.e.*, the riders who temporarily rent the devices).²⁵
- Fourth, requiring access to geolocation information as a condition of receiving a permit constitutes compelling the production of or access to electronic device information, consistent with the California Legislature’s intent in enacting

²⁰ “‘Electronic device information’ means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.” Cal. Pen. Code § 1546(g).

²¹ “‘Electronic information’ means electronic communication information or electronic device information.” Cal. Pen. Code § 1546(h).

²² “‘Authorized possessor’ means 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.*” Cal. Pen. Code § 1546(b) (emphasis added).

²³ See Attachment A, pp. 2–3.

²⁴ See Attachment A, p. 5.

²⁵ See Attachment A, p. 5.

CalECPA of strengthening and expanding existing Fourth Amendment protections and creating a “clear, uniform warrant rule.”²⁶

Legislation limiting local authorities to aggregated and deidentified trip data for city and regional planning purposes will help avoid further conflicts with not only CalECPA, but also the U.S. Supreme Court’s recent holding in *Carpenter v. United States*, which requires a warrant before the government can gain access to historical location data. *See Carpenter*, 138 S. Ct. at 2221 (“the Government must generally obtain a warrant supported by probable cause before acquiring” location records).

— — —

Local authorities should have the right to regulate the use of TNCs and shared mobility devices. However, those efforts should not undermine California riders’ right to privacy. EFF supports legislative efforts that strike the right balance between the need to protect individual privacy and the need for local authorities to obtain the data they need for planning purposes—by limiting local authorities to aggregated and deidentified trip data.

Respectfully Submitted,



Jamie Williams
Staff Attorney
Electronic Frontier Foundation
(415) 436-9333 x164
jamie@eff.org

CC: Honorable Members of the California Legislature; Governor’s Office of California

²⁶ *See* Attachment A, pp. 6–7.

Attachment A



CHIEF DEPUTY
Aaron D. Silva

PRINCIPAL DEPUTIES
Joe Avala
Sergio E. Carpio
Amy Jean Havdt
Thomas J. Kerbs
Kirk S. Louie
Fred A. Messerert
Gerardo Partida
Robert A. Pratt

LEGISLATIVE
COUNSEL
BUREAU

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

August 1, 2019

Stephen G. Dehrer
Lisa C. Goldkuhl
Daniel J. R. Kessler
William F. Moddelmog
Sheila R. Mohan
Natalie R. Moore
Robert D. Roth
Michelle L. Samore
Daniel Vandekoolwyk

Honorable Jacqui Irwin
Room 5119, State Capitol

CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT - #1916004

DEPUTIES
Judy Anne Alams
Paul Arata
Jennifer Klein Baldwin
Jeanette Barnard
Jennifer M. Barry
Vanessa S. Bedford
Robert C. Binning
Brian Bitzer
Rebecca Bitzer
Julia Blair
Brian Bobb
Lucas Botello
Ann M. Burastero
William Chan
Flame Chu
Paul Coaxum
Thomas Dombrowski
Roman A. Edwards
Sharon E. Everett
Kirsta M. Ferns
Jessica S. Gosney
Nathaniel W. Grader
Ryan Greenlaw
Matt C. Guzman
Romyn Hamed-Troyansky
Jacob D. Heninger
Alex Hirsch
Stephanie Elaine Hoehn
Russell H. Holder
Cara E. Jenkins
Valerie R. Jones
Lori Ann Joseph
David B. Judson
Alyssa Kaplan
Amanda C. Kelly
Jessica D. Kenny
Christina M. Kenzie
Michael J. Kernis
Mariko Kotani
Christopher LaGrassa
Felicia A. Lee
Kathryn W. Londenberg
Daniela N. Lopez Garcia
Adam Maas
Richard Malnic
Anthony P. Marquez
Aimee Martin
Francisco Martin
Amanda Mattson
Abigail Maurer
Lindsey S. Nakano
Yoeli Chor O'Brien
Christine Paxinos
Sue Ann Peterson
Lisa M. Plummer
Stacy Sacchao
Kevin Schmitt
Amy E. Schweitzer
Melissa M. Scolari
Jessica L. Steele
Anton C. Swain-Gil
Mark Franklin Terry
Joanna E. Varner
Bradley N. Webb
Rachelle M. Weed
Brent W. Westcott
Aruni G. Yazdi

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[ing] the production of or access to electronic communication information from a service provider," (2) "Compel[ing] 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 reh. 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[ing] 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