Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 523 (Irwin) – As Introduced February 13, 2019

SUBJECT: Telecommunications: customer right of privacy

SUMMARY: This bill would prescribe the circumstances under which telephone and telegraph corporations may release customer proprietary network information (CPNI), or specified information that is *not* included in CPNI, regarding noncommercial subscribers without their written consent. This bill would add geolocation information, as defined, to the list of non-CPNI that may only be released with a noncommercial subscriber's written consent. The bill would separately permit a telephone corporation to share the CPNI of a subscriber with its agents and affiliates that provide communications-related services for the purpose of marketing communications-related services to that subscriber if the telephone corporation obtains the written consent of the subscriber or if the telephone corporation does not receive an objection pursuant to a specified federal opt-out approval mechanism. Specifically, **this bill would**:

1) Prohibit any telephone or telegraph corporation from making available to any other person or corporation, without first obtaining a noncommercial subscriber's written consent, CPNI of the noncommercial subscriber or the geolocation information of the noncommercial subscriber.

2) Define "geolocation information" to mean information related to the physical or geographical location of a noncommercial subscriber or the noncommercial subscriber's communications device, regardless of the particular technological method used to obtain this information.

3) Add additional exemptions to the written consent requirement before telephone companies release specified information, including CPNI and geolocation information as added above, for the following:

    - Information required to deliver mobile telephony service to the noncommercial subscriber.

    - Information required during a customer-initiated transaction to effectuate a change in the mobile telephony service of the noncommercial individual subscriber.

4) Specify that, subject to obtaining the express written consent or federal opt-out approval of the subscriber, a telephone corporation may share CPNI of a mobile telephony services subscriber with its agents and affiliates that provide communications-related services for the purpose of marketing communications-related services to that subscriber.

5) Define various terms, in addition to "geolocation information," for these purposes, including:

    - "CPNI" to mean customer proprietary network information as defined under federal law and as interpreted by the Federal Communications Commission (FCC), as specified.

- "Federal opt-out approval" to mean the "opt-out approval" method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI adopted by the FCC, as specified.

EXISTING LAW:

1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art., Sec. 1.)

2) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

   - the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI, and the specific pieces of information collected about the consumer;

   - the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;

   - the right to access the specific pieces of information a business has collected about the consumer;

   - the right to delete information that a business has collected from the consumer;

   - the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and,

   - the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

3) Generally requires under the CCPA that a business subject to the CCPA do all of the following, among other things: comply with the above requirements, provide various notices to those ends, and execute various requests upon receipt of a VCR, as specified; and provide certain mechanisms for consumers to make their lawful requests, including a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's internet homepage to enable consumers, or a person authorized by the consumer, to opt-out of the sale of the consumer's PI. (Civ. Code Sec. 1798.100 et seq.)

4) Grants all consumers over the age of 16 the right, at any time, to direct a business that sells PI about the consumer to third parties not to sell the consumer's PI (the right to "opt-out"). For all consumers less than 16 years of age, prohibits businesses from selling PI unless the consumer (or in the case of consumers under 13 years of age, the consumer's parent or guardian) has affirmatively authorized the sale of the consumer's PI (the right to "opt-in"). (Civ. Code Sec. 1798.120.)

5) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill, defines the following terms:

- "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' PI, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' PI, that does business in California, and that satisfies one or more of certain thresholds relating to the business's revenue, among other things.

- "PI" generally 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. PI includes certain specific types of information, if that information identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. Of importance for this bill, this list includes geolocation data.

- "Sell," "selling," "sale," or "sold," generally means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to another business or a third party for monetary or other valuable consideration. (Civ. Code Sec. 1798.140.)

6) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, consent of the owner of the device, or emergency situations, as specified. (Pen. Code Sec. 1546 et seq.)

7) Defines CPNI, as a matter of federal law, to mean: (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and, (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that such term does not include subscriber list information. (47 U.S.C. Sec. 222.)

8) States, as a matter of federal regulations:

- Instances in which a telecommunications carrier can use the CPNI without customer approval. The authorized circumstances include, among other things, where the carrier provides inside wiring installation, maintenance, and repair services, as well as for the purpose of conducting research on the health effects of CMRS [Commercial Mobile Radio Service]. (47 C.F.R. Sec. 64.2005.)

- A carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under [Section] 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval. (47 C.F.R. Sec. 64.2007.)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks to protect Californians' privacy with respect to the sale of their geolocation information by telephone corporations. This is an author-sponsored bill.

2) **Author's statement**: According to the author, "[c]urrently California law relating to Customer Proprietary Network Information (CPNI), including geo-location of mobile phone users, lags behind federal law and [Federal Communications Commission] FCC regulations. With recent reports of the sale and misuse of mobile phone users geo-location, and the lack of enforcement by the FCC of federal protections, AB 523 updates California law to give Californians a state law remedy to the misuse of their geo-location information. This bill expands current state law protections of CPNI by 1) changing 'residential' subscriber to 'noncommercial' subscriber to incorporate mobile phone subscribers into the protections of PUC 2891, 2) incorporate by reference all information the FCC has decided constitutes CPNI into the protections of PUC 2891[,] 3) explicitly includes geo-location as a protected piece of CPNI[, and] 4) provides definitions of terms linking them to federal statutes and FCC regulations, and incorporates certain functional exemptions that exist in federal law."

3) **Protections for CPNI**: This bill contains many of the same provisions of another bill, AB 3011 (Huffman, 2008) with respect to its treatment of CPNI. Under federal law, "CPNI" means "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information." (47 U.S.C. Sec. 222.) "Subscriber list information," in turn, means information: (A) identifying the listed names of a carrier's subscribers and such subscribers' telephone numbers, addresses, or primary advertising classifications, or any combination of such listed names, numbers, addresses, or classifications; and, (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format. (*Id*.)

The only substantive difference between AB 3011 and this bill is the express inclusion of "geolocation information" and the corresponding definition for that term in AB 523. As noted in the Assembly Utilities and Commerce Committee analysis at that time:

> Existing state and federal laws seek to protect telephone customers' privacy by prohibiting telephone companies from sharing information about their subscribers with their affiliates or with third parties without obtaining the subscriber's consent. The protected information is generally referred to as Consumer Proprietary Network Information (CPNI).
>
> California's privacy rules contain a broader definition than federal rules of what information is consider private. The federal CPNI rules protect information that relates to the type and number of telephone calls a subscriber makes, while the California statute also protects credit and other personal financial information of the subscriber.
>
> Prior to January 2008, the federal CPNI rules allowed telephone companies to share CPNI with their agents, affiliates, joint venture partners and independent contractors unless the customer "opts-out." To opt-out a customer must actively object to the sharing of her information after the telephone company notifies the customer of the opportunity to object. If the customer fails to object, the information can be shared.
>
> California law prohibits telephone companies from sharing CPNI and financial information unless the customer opts-in. To opt-in the customer must provide the telephone company with expressed written consent to share the information.
>
> In response to numerous incidents of unauthorized sharing of CPNI, the Federal Communications Commission (FCC) tightened its CPNI rules in 2007. After January 2008, federal rules prohibit the sharing of CPNI unless the telecommunications company:
>
> a) Obtains prior opt-in consent of the subscribers before sharing CPNI with independent contractors or joint venture partners for outbound telemarketing of services.
> b) Obtains opt-out consent before sharing information with affiliate companies for the marketing of services to which the customer does not already subscribe.
> c) Authenticates that an actual subscriber is requesting access to protected information before the information is released to the subscriber.
> d) Protects a subscriber's CPNI even when it is outside the provider's immediate control.
> e) Takes "every reasonable effort" to prevent the unauthorized discloser of a subscriber's CPNI.
>
> While the FCC CPNI rules do not apply to financial and credit information, the Federal Fair Credit Reporting Act (FCRA) does limit the ability of telephone companies to share financial information they have gained through credit reports. However, the FCRA allows the companies to share the credit information with opt-out consent, while California rules require customers to affirmatively opt-in before their information can be shared. Additionally, the federal rules generally only apply to financial information that is obtained through credit reports, where California law applies all financial information no matter how it is obtained. (*See* Asm. Utilities and Commerce Com., analysis of AB 3011 (2007-2008 Reg. Session), May 22, 2018, p. 2.)

The problem that AB 3011 sought to address was largely that mobile telephone companies had interpreted California's privacy laws to apply only to residential landline customers. "While the history of the statute appears to show that the 'residential' customer's language was intended to create a distinction between business customers and customers that use the telephone for personal use, the [Public Utilities Commission] and some mobile telephone companies are beginning to interpret California's telephone rules as only applying to residential landline customers. Because mobile telephone companies do not distinguish between residential and non-residential customers, the mobile telephone companies believe they are not subject to California's telephone privacy rules." (*Id.* at 3.) This bill, like AB 3011, would resolve that issue by replacing references to "residential" subscribers with "noncommercial" subscribers. Also similar to AB 3011, this bill contains provisions that would allow telecommunications companies to share CPNI information with affiliate companies with opt-out consent (consistent with the FCC rules), as opposed to the "opt-in" consent currently required.

Of particular relevance for this Committee, staff notes that while the federal definition of CPNI would appear to cover geolocation information, this bill includes "geolocation information" separately within an enumerated list of "information that is not included in CPNI." As such, because the provision requiring telephone companies to receive either written consent or "federal opt-out approval" applies to limit these companies' ability to "share CPNI of a mobile telephony services subscriber," it appears that this provision of the bill would not apply to the information that falls under the enumerated list – including geolocation information. Indeed, much of the information that is listed under the phrasing of "information that is not included in CPNI" would otherwise appear to constitute CPNI under federal law. Accordingly, as with "geolocation information," those items would presumably be subject to "opt-in" written consent and could not otherwise be shared with agents or affiliates. That being said, this may be an unintended consequence of how the bill has technically been drafted. Indeed, if the author's intent is to apply "written consent or federal opt-out approval" to geolocation information as well, the author may wish to clarify the bill to avoid this potentially erroneous interpretation. (*See* Comment 6 for more.)

4) **New York Times recently detailed how "anonymized" geolocation data tracks individuals and reveals intimate, private details of a person's life**: A December 2018 New York Times article, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, highlights this issue with alarming detail:

> The millions of dots on the map trace highways, side streets and bike trails — each one following the path of an anonymous cellphone user.
>
> One path tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour. Another represents a person who travels with the mayor of New York during the day and returns to Long Island at night.
>
> Yet another leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her.
> An app on the device gathered her location information, which was then sold without her knowledge. It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The

> New York Times. While Ms. Magrin's identity was not disclosed in those records, The Times was able to easily connect her to that dot. The app tracked her as she went to a Weight Watchers meeting and to her dermatologist's office for a minor procedure. It followed her hiking with her dog and staying at her ex-boyfriend's home, information she found disturbing. […]
>
> Like many consumers, Ms. Magrin knew that apps could track people's movements. But as smartphones have become ubiquitous and technology more accurate, an industry of snooping on people's daily habits has spread and grown more intrusive. (Valentino-DeVries, Singer, Keller and Krolik, New York Times (Dec. 10, 2018).)

An interactive map on the online publication of this article demonstrates exactly how this is possible. As explained in that map, connecting a dot from one location (her home) to another location (a school), "Lisa Magrin is the only person who travels regularly from her home to the school where she works. Her location was recorded more than 800 times there, often in her classroom." (*Id*.) As described in that article:

> At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information, The Times found. Several of those businesses claim to track up to 200 million mobile devices in the United States — about half those in use last year. The database reviewed by The Times — a sample of information gathered in 2017 and held by one company — reveals people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day.
>
> These companies sell, use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It's a hot market, with sales of location-targeted advertising reaching an estimated $21 billion this year. […]
>
> Businesses say their interest is in the patterns, not the identities, that the data reveals about consumers. They note that the information apps collect is tied not to someone's name or phone number but to a unique ID. But those with access to the raw data — including employees or clients — could still identify a person without consent. They could follow someone they knew, by pinpointing a phone that regularly spent time at that person's home address. Or, working in reverse, they could attach a name to an anonymous dot, by seeing where the device spent nights and using public records to figure out who lived there. (*Id*.)

5) **CCPA covers precise geolocation information**: As drafted, this bill appears to require opt-in written consent before a telephone company can make a noncommercial subscriber's geolocation data available to any other person or corporation. For these purposes, geolocation data means any information related to the physical or geographical location of a noncommercial subscriber or the noncommercial subscriber's mobile communications device, regardless of the particular technological method used to obtain this information.

   Last year, the Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their PI, such as: (1) the right to know what PI that is collected and sold about them; (2) the right to delete PI collected from them; and, (3) the right to opt-out of the sale of their PI, or opt-in for minors under 16 years of age.

Under the CCPA, all consumer rights and the businesses' corresponding obligations, are dependent upon whether or not certain data constitutes "PI." Generally speaking, the CCPA defines PI as that information which identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (*See* Civ. Code Sec. 1798.140(o)(1).) The CCPA definition of PI then proceeds to include a list of items that are deemed "PI," but *only* insofar as those items "identify, relate to, describe, are capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." Of particular importance to this bill, that list includes "geolocation information." Also of importance to this bill is that the CCPA exempts "deidentified" or otherwise "aggregate consumer information" from the definition of PI.[1] While such anonymization-based requirements provide privacy protection under the CCPA, as evidenced by the December 2018 NYT article discussed above, there is reason to believe that when it comes to the nature of geolocation data, even where the information has been "anonymized," it can readily identify a particular individual. Recognizing the heightened potential for privacy intrusions with geolocation data, this bill presents a question as to whether the "opt-out" right for consumers 16 years of age and over should be an "opt-in" right in this particular instance.

As such, requiring "opt-in" for the sharing of geolocation data by a telephone company with other persons or entities, would arguably be appropriate and consistent with other California law. Specifically, the CalECPA recognizes that government cannot intrude on a person's privacy by obtaining this type of electronic communication information from service providers or electronic device information from any other person or third party who is not the authorized possessor of the device, absent a warrant or in other limited circumstances. Nor can government simply access that electronic device information by means of physical interaction or electronic communication, without meeting similar requirements. The information protected by these CalECPA provisions includes geolocation data from a device.[2] Given that there is such a clear line, consistent with the Fourth Amendment of the

---

[1] Though there is a drafting error in that provision, two bills this year seek to correct that error to ensure the CCPA accurately reflects these exemptions from the definition of PI. (*See* AB 874 (Irwin) and AB 1355 (Chau).)

[2] Indeed, in 2017, the U.S. Supreme Court was faced with a question of how the Fourth Amendment applies "to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals" in the case of *Carpenter v. United States* (2018) 138 S. Ct. 2206. The Court distinguished *Carpenter* from prior cases dealing with third party doctrine (a doctrine stating that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties), because cell phone location is not truly "shared" voluntarily by a person, as one usually understands that term. Indeed, a cell phone logs a cell-site record without any affirmative act on the part of the user beyond powering up, and "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." (*Id*. at 2220). The Court emphasized that historical cell-site records present even greater concerns than the GPS monitoring of a vehicle considered in *Jones* because, unlike the bugged container in *United States v. Knotts* (1983) or the car in *United States v. Jones* (2012), a cell phone is practically a feature of human anatomy in how it "tracks nearly exactly the movements of its owner." "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." (*Id*. at 2218.) Importantly, the Court found significance in the retrospective quality of the data that police could access, noting that it gives police access to a category of information otherwise unknowable when attempting to reconstruct a person's movements – which in the past were "limited to a dearth of records and the frailties of recollection." This retroactive quality was important to the holding, because it left open the question of how the Court might interpret a case involving the *real-time collection* of that same cell-site location records (CSLI). The Court expressly states in Carpenter, that its "decision today is a narrow one. [The Court] do[es] 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 cite during particular interval)."

U.S. Constitution and Article 1, Section 1 of the State Constitution, precluding unreasonable governmental intrusion into individuals' right of privacy in this information by effectively preventing private entities from simply handing the data to law enforcement at will, it is unclear why these private entities should be able to share it with one another, without the person's affirmative "opt-in" consent.

That being said, to avoid confusion, if it is the author's intent to replace the CCPA's "opt-out" provision for telecommunications carriers, the author may wish to expressly amend this bill, or add an amendment to Section 1798.125 of the Civil Code (delineating the CCPA's opt-out/opt-in rights) within this bill, to recognize that the opt-in right of this bill supersedes the opt-out right of the CCPA for geolocation information in the possession of telecommunications carriers.

On the other hand, if the intent of the author is to require *either* ("opt-in") written consent, or "federal opt-out approval" for geolocation information, there may be greater confusion as to how the law will interact with the CCPA and what "federal opt-out approval" means, as discussed further in Comment 6, below.

6) **"Federal opt-out approval" and the CCPA**: Questions have been raised about the interplay of this bill with the CCPA with respect to geolocation data, in particular. To be clear, the only overlap that exists would be with respect to how *telephone companies* handle certain types of information relating to their subscribers, that might otherwise be PI – including, but not limited to, geolocation information. Stated another way, insofar as the bill attempts to incorporate federal law and corresponding rules regarding CPNI into California law, those federal regulations only restrict the behavior of the telecommunications carriers and this bill only applies to telephone and telegraph corporations. They do not apply to other businesses that make applications available on a phone to consumers and thereby collect, use, or share the users' GPS data.

   As noted above, as currently drafted, this bill appears to require "opt-in" approval by way of written consent for the sharing of geolocation data by a telephone corporation with any other person or corporation. At the same time, however, it appears that the author's intent is to require *either* ("opt-in") written consent or what the bill terms "federal opt-out approval," for CPNI. Indeed, background material submitted to Committee suggests that the author interprets geolocation information as a type of CPNI that is subject to "federal opt-out approval" in some instances – whereas the drafting of this bill suggests geolocation information is "information that is not included in CPNI" and subject to the subscriber's written consent before a telephone company could ever share that information. As such, first and foremost, if the intent of the author is to include geolocation information as a form of CPNI which is subject to "federal opt-out approval" in some instances, the bill needs to be clarified to achieve that intent.

   Notably, the issue of needed clarity, however, is not limited just geolocation data. The applicable mechanism for protecting a subscriber's privacy in CPNI or enumerated non-CPNI that otherwise meet the CCPA's definition of PI, should be further clarified as well. In background submitted to Committee, the author writes that:

   > While the scope and definitions of the CCPA and applicable federal law are not harmonious, in most regards the same information that would be considered 'Personal Information' under CCPA would be CPNI. To the extent other CCPA definitions, like

that of 'business' are met by telecommunications carriers, the scope of CCPA would supplement the FCC rules. The CCPA right to opt-out of the sale of personal information is the most analogous to the protections of federal law that this bill is trying to create a parallel state enforcement mechanism.

The manner in which the CCPA will regulate the sale of CPNI though diverges from the Communications Act of 1934, FCC regulations, and FCC rulings that in general require opt-in consent of the user for CPNI usage. There is a list of uses of CPNI that the FCC has enumerated to not need customer consent (47 CFR 64.2005), and then another enumerated list of uses that may be undertaken by following an "opt-out approval" that requires notice and a minimum 30-day election period (47 CFR 64.2007(b)), but the default is opt-in consent for all non-enumerated uses.

[…] To lawfully sell CPNI, including sale of residential subscriber's demographic information, federal law would require opt-in consent to a telecommunications provider, this is also the case in PUC 2891, but the CCPA would not be triggered unless a consumer had previously opted-out. [Under this bill, if] a sale did occur, the California consumer's federal rights would be violated and could petition the FCC to bring an enforcement action against the telecommunications provider, their California right under PUC 2891 would be violated and they could bring a civil suit own their own behalf, if they had opted-out previously their California rights would also be violated and could petition the AG to bring an enforcement action against the telecommunications provider. If they had not opted-out they would have no recourse under CCPA, but could prospectively opt-out of future sale.

The types of legal recourse are narrowed though when you apply current law to a mobile phone subscriber, or to geo-location information. To lawfully sell CPNI, including sale of mobile phone subscriber's geo-location information, federal law would require opt-in consent to a telecommunications provider, but it is not currently covered by PUC 2891, and the CCPA would not be triggered unless a consumer had previously opted-out. If a sale did occur, the California consumer's federal rights would be violated and could petition the FCC to bring an enforcement action against the telecommunications provider, [but] **their California right under PUC 2891 in statute today would not be violated and they could not bring a civil suit own their own behalf**, [though] if they had opted-out previously their California rights would also be violated and could petition the AG to bring an enforcement action against the telecommunications provider. If they had not opted-out they would have no recourse under CCPA, but could prospectively opt-out of future sale.

With information on mobile phone subscribers and geo-location information more sensitive than information on the dwindling numbers of residential subscribers and their demographic information, the additional remedy embodied in PUC 2891 should be available for more sensitive information if it continues to be available for less sensitive information.

Ultimately, assuming that this bill would supersede the CCPA with respect to PI that is CPNI and subject to written consent or "federal opt-out approval" as well as with respect to non-CPNI information subject to "written consent," a question arises as to what "federal opt-out approval" means. The bill currently defines "federal opt-out approval" to mean the "opt-out

approval" method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI adopted by the FCC in Subpart U (47 C.F.R. Sec. 64.2001 et seq.) That part of the federal regulations, however, is rather unclear as it does not appear to have a singular definition that would readily translate here to provide clear direction as to when written consent is needed and when opt-out applies.

Indeed, in one area, the regulations that a telecommunications carrier "may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer" – not specifying which consent mechanism applies, or whether it is at the election of the carrier. (*See* 47 C.F.R. Sec. 64.2007(b).) As such, it is not entirely clear in what instances this bill would allow for opt-out, as opposed to opt-in rights. If this Committee were to approve this bill and, if the author intends to apply the provision allowing for "federal opt-out approval" to geolocation data, the author may wish to not only provide clarity to that end, but also provide additional clarity as to what scenarios require "federal opt-out approval" as opposed to written consent.

7) **Arguments in support**: The Public Advocates Office (office) in the California Public Utilities Commission writes in support of this bill as it "would strengthen privacy protections for customers of telephone corporations, including wireless carriers." The office writes:

> This bill would require wireless carriers to obtain written consent from their customers before they share or sell a customer's real-time location information to other individuals or businesses. This is important because recent investigations have demonstrated that wireless carriers have been selling highly-accurate, real-time customer location data to companies who resell the information to other companies without obtaining a customer's consent. We support this bill because it would help put an end to this practice and strengthen privacy protections that customers deserve.
>
> AB 523 also would exempt wireless carriers from having to obtain written consent from customers when customer information is shared with public safety agencies during an emergency. This exemption is reasonable during an emergency situation. (Footnote omitted.)

8) **Support if amended**: Consumer Reports writes a "support if amended" letter to this bill, indicating that "strongly support[s] the effort to extend stronger privacy protections to cell phone data and geolocation data. While the California Consumer Privacy Act (CCPA) protects the sale of geolocation data on an opt-out basis, AB 523 ensures even stronger protections, by securing privacy by default with respect to this data. This is important, particularly in light of recent reports that cell phone carriers such as T-Mobile, Sprint, and AT&T, have been selling this data to third parties, suggesting that these protections are long overdue. The sale and resale of this information could allow broad access to the consumer's physical location." To "improve" the bill, however, it requests that the author "address certain overbroad exemptions" as follows:

> For example, Section 2891(e) is confusing: "Subject to obtaining the express written consent or federal opt-out approval of the subscriber, a telephone corporation may share CPNI of a mobile telephony services subscriber with its agents and affiliates that provide communications-related services for the purpose of marketing communications-related

services to that subscriber." It is unclear from this language whether a consumer has to opt in or opt out of such communications, which could potentially subject consumers to unwanted marketing messages without their permission and compromise consumer privacy. To address this, you should delete this provision from the bill, since consumers may already agree to such sharing under the bill. The exemptions for the use of information to deliver and make a change to the telephone service in Section 2891(d)(12)-(13) should be more tailored as well, for example by clarifying that the exemptions apply only to those services specifically requested by consumers.

Media Alliance also writes in a "support if amended" letter that "[t]he need for the protection of CPNI and geolocation data is evident from the series of news stories in 2018 regarding the collection of geolocation data from mobile devices even when customers turned off location tracking on their devices, presumably intending to withhold their consent. […] However, we have concerns about the intersection of this bill's much-needed stronger protections with the California Consumer Privacy Act of 2018. […] [AB] 523 takes two approaches to providing enhanced protection for the classes of data identified in the bill as particularly sensitive. Firstly, it imposes an opt-in standard (pending any federal legislation), rather than the opt-out standard that applies globally to all personal information in CCPA." To this end, Media Alliance raises concerns underlying its conditional support, including the following:

> While the categories of data identified in this bill are definitely extremely sensitive, they are not only and exclusively the sole categories of personal information that should be defined as extremely sensitive and subject to enhanced protections. To give some examples, biometric data such as voice prints and face prints, retina imagery and DNA profiles are certainly as or more sensitive as calling patterns and geolocation data. We also note that geolocation data is collected by other parties and by other means within the state than telephone and telegraph corporations, including automated license plate readers, which are in common use by both law enforcement agencies and private actors throughout California.

To that end, Media Alliance seeks for the author to consider whether to follow a more "holistic" approach is appropriate similar to AB 561 (Jackson) and AB 1760 (Wicks).

9) **Arguments in opposition**: CTIA, representing a coalition of telecommunications providers including AT&T and Verizon, submits an "oppose unless amended" letter stating that: (1) AB 523 is unnecessary because the CCPA already provides rights and obligations related to consumers' geolocation data; (2) AB 523 will cause consumer confusion; and (3) AB 523 should limit the affirmative opt-in requirements to precise geolocation data. Specifically, CTIA writes:

- The CCPA provides consumers with strong privacy rights over their [PI], including geo-location data. For example, the CCPA provides access and deletion rights and the right to opt-out of the sale of [PI]. Companies are required to provide consumers with clear and conspicuous notice of these opt-out rights.

- The CCPA applies equally to all businesses that meet its thresholds. Imposing different obligations that depend on the type of business holding the data would cause consumer confusion, distort competition, and create difficult implementation challenges. For example, consider a consumer who opts in to sharing geo-location information under AB

523, but had opted out of sale of their [PI] under the CCPA (Cal. Civ. Code [Sec.] 1798.120). It would be difficult, if not impossible, for a business to ascertain consumers' intentions. […]

- AB 523's definition of "geo-location" is very broad and will sweep in the types of information that raise little or no privacy concerns. Information about a user's city, state, or region is potentially subject to AB 523's opt-in requirement. Such information cannot be used, as a practical matter, to physically locate an individual, yet it could be covered if it is "related to the physical or geographical location" of the subscriber. Opt in should apply only to precise geolocation data in concert with FTC policy deeming such data sensitive. (Subheadings and footnote omitted.)

10) **Concern letter with request for amendment**: MuniServices writes a letter of concern because it believes that this bill would severely limit a local government's access to the information needed to perform an audit of a telephone Utility Users Tax (UUT) collections. The issue MuniServices raises applies to the portion of the bill dealing with CPNI disclosures by a telephone company without the subscribers written consent. Again, this law applies generally to landline companies, as described in Comment 3 above, and under this bill would also apply to mobile telephone companies, while limiting the sharing of CPNI data by a telephone company with its agents or affiliates. MuniServices writes:

    To perform a UUT audit, local governments do not need individually identifying information about customers (e.g. name); but they do need the actual billing charges contained in customers' bills. MuniServices is concerned that customers' billing charges would fall within the definition of CPNI because they potentially relate to the type and amount of use. Local governments need this information because UUTs are based on the taxable charges contained in a telephone bill, and not all charges are taxable. Therefore, a local government needs to be able to review the individual charges of customers' telephone bills to ensure that telephone companies are properly calculating and remitting its tax. If this information falls within the definition of CPNI, AB 523, as currently written, would prohibit a telephone company from providing the information to a local government that is conducting an audit without the written consent of each customer (Pub. Util. Code [Sec.] 2891(a)), which would virtually prohibit audits; and audits are the only way for local governments to ensure that UUTs are being properly collected and remitted[.]

    To address this problem, MuniServices proposes adding a subsection (14) to subdivision (d) of section 2891. Subdivision (d) lists the types of information to which the privacy protections of section 2891 do not apply, and the proposed subsection (14) would state that these protections do not apply to "information provided to a local government by a telephone company for an audit or inspection of the telephone company's records for the collection of a tax, fee, or other charge by the local government." The goal of this amendment is to protect local governments' ability to review and audit telephone company records to ensure accurate collection of utility users taxes, while not hindering the purpose of the bill, which is to prohibit the unauthorized selling or sharing of customer data.

11) **Related legislation**: AB 25 (Chau) seeks to clarify the CCPA's definition of consumer and how businesses may comply with a consumer's request for specific pieces of information in a

privacy protective manner under the CCPA. This bill is pending hearing in the Assembly Appropriations Committee.

AB 288 (Cunningham) seeks to establish laws governing "social media privacy" separately from the CCPA's existing requirements for such companies that meet the "business" definition thresholds identified in the CCPA. Specifically, the bill would require a social networking service, as defined, to provide users that close their accounts the option to have the user's "personally identifiable information" permanently removed from the company's database and records and to prohibit the service from selling that information to, or exchanging that information with, a third party in the future, subject to specified exceptions. The bill would authorize consumers to bring private right of action for a violation of these provisions, as specified. This bill has been referred to this Committee.

AB 846 (Burke) seeks to replace "financial incentive programs" provisions in the non-discrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified. This bill is pending hearing in the Assembly Appropriations Committee.

AB 873 (Irwin) seeks to revise the CCPA's definitions of "PI" and "deidentified" and to revise the CCPA's existing provision that prohibits the act from being construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. This bill is pending hearing in the Assembly Appropriations Committee.

AB 874 (Irwin) seeks to revise the definition of "publicly available" for purposes of the PI definition, which excludes such information. The bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information. This bill is pending hearing in the Assembly Appropriations Committee.

AB 981 (Daly) would add numerous privacy protections to the Insurance Information and Privacy Protection Act (IIPPA), to reflect the CCPA. The bill would exempt entities subject to the IIPPA, as specified, from the CCPA, with the exception of the CCPA's data breach section. This bill is pending hearing in the Assembly Appropriations Committee.

AB 1035 (Mayes) seeks to require, under the Data Breach Notification Law, a person or business, as defined, that owns or licenses computerized data that includes PI to disclose any breach of the security of the system within 72 hours following discovery or notification of the breach, subject to the legitimate needs of law enforcement, as provided. This bill is pending hearing in this Committee.

AB 1138 (Gallagher) seeks to prohibit a person or business that conducts business in California, and that operates a social media website or application, from allowing a person under 13 years of age to create an account with the website or application unless the website or application obtains the consent of the person's parent or guardian before creating the account. This bill is pending hearing in the Assembly Appropriations Committee.

AB 1146 (Berman) seeks to expand the CCPA exemptions to expressly exclude from the CCPA vehicle information shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared pursuant to, or in anticipation of, a vehicle repair

relating to warranty work or a recall, as specified. This bill is pending hearing in the Assembly Appropriations Committee.

AB 1355 (Chau) seeks to address a drafting error in the definition of PI to clarify that it does not include deidentified or aggregate consumer information. This bill is pending hearing in the Assembly Appropriations Committee.

AB 1395 (Cunningham) seeks to prohibit a smart speaker device, as defined, or a specified manufacturer of that device, from saving or storing recordings of verbal commands or requests given to the device, or verbal conversations heard by the device, as specified. This bill is pending hearing in this Committee.

AB 1416 (Cooley) seeks to expand various CCPA exemptions. This bill is pending hearing in this Committee.

AB 1564 (Berman) would revise a CCPA requirement that businesses make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA, including a toll-free telephone number. This bill is pending hearing in the Assembly Appropriations Committee.

AB 1760 (Wicks) would restate the CCPA rights using similar terminology, expand those existing CCPA rights to include new rights, and replace the "opt-out" rights of consumers 16 years and older with an "opt-in" right, among other things. This bill has been referred to this Committee.

12) **Prior legislation**: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment 3.

AB 3011 (Huffman, 2008) *See* Comment 3. That bill failed passage on the Assembly Floor.

13) **Double-referral**: This bill was double-referred to the Assembly Communications and Conveyance Committee where it was heard in April 24, 2019, and passed on a 9-2 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

Public Advocates Office
Consumer Reports (if amended)
Media Alliance (if amended)

Opposition

AT&T Inc. and its affiliates (unless amended)
CTIA-The Wireless Association (unless amended)
Sprint Corp (unless amended)
T-Mobile USA, Inc. (unless amended)
Tracfone Wireless, Inc. (unless amended)
Verizon Communications, Inc. and its affiliates (unless amended)

Analysis Prepared by: Ronak Daylami / P. & C.P. / (916) 319-2200