SENATE COMMITTEE ON ENERGY, UTILITIES AND COMMUNICATIONS
Senator Ben Hueso, Chair
2019 - 2020 Regular

Bill No:	AB 523	**Hearing Date:**	7/2/2019
Author:	Irwin		
Version:	5/20/2019 As Amended		
Urgency:	No	**Fiscal:**	No
Consultant:	Sarah Smith		

SUBJECT: Telecommunications: customer right of privacy

DIGEST: This bill adds subscribers' customer proprietary network information (CPNI) to list of information a telephone corporation is prohibited from disclosing without first obtaining subscribers' written consent and includes a subscriber's geolocation information in the definition of CPNI.

ANALYSIS:

Existing law:

1) Prohibits telephone corporations from disclosing certain subscriber information without first obtaining consent, including, but not limited to calling patterns, demographic information, a subscriber's credit or other personal financial information, and services purchased by a subscriber. (Public Utilities Code §2891(a))

2) Establishes exemptions to the prohibition on telephone corporations' sharing of subscriber information, including, but not limited to, disclosures needed for 911 purposes and pursuant to a law enforcement lawful process. (Public Utilities Code §2891(d))

3) Prohibits wireless telecommunications providers and their affiliates from disclosing the name and telephone number of a subscriber unless the subscriber expressly provides consent for the disclosure. (Public Utilities Code §2891.1(b))

4) Allows a subscriber to revoke a prior authorization to disclose subscriber information at any time. Wireless telecommunications providers must comply with a revocation within 60 days. (Public Utilities Code §2891.1(d))

5) Exempts the following purposes from prohibitions on disclosing telecommunications subscribers' phone numbers:

a) Disclosures to a collection agency, exclusively for the collection of unpaid debts and subject to supervision by the California Public Utilities Commission (CPUC).
b) Disclosures to a law enforcement agency, fire protection agency, public health agency, public environmental health agency, city or county emergency services planning agency, or private for-profit agency contracting with one or more of these agencies, for the exclusive purpose of responding to a 911 call or communicating an imminent threat to life or property.
c) Disclosures pursuant to a lawful process issued under state or federal law.
d) Disclosures to a telephone corporation providing service between service areas for service in those areas or to third parties for the limited purpose of billing.
e) Disclosures to a telephone corporation to effectively transfer telephone service to a new provider.
f) Disclosures to the CPUC pursuant to its regulatory authority. (Public Utilities Code §2891.1(f)).

6) Specifies that any deliberate violation of prohibitions to disclosures of telecommunications subscriber information is grounds for a civil suit against the entity responsible for the violation. (Public Utilities Code §2891.1(g))

This bill:

1) Adds CPNI to the list of subscriber information a telephone corporation is prohibited from disclosing without first obtaining written consent from the subscriber.

2) Specifies that CPNI includes the following information:
   a) The subscriber's calling patterns.
   b) Services purchased by the subscriber from the telephone corporation or an information services provider that delivers services through the telephone line.
   c) Demographic information about the subscriber or aggregate information from which individual identities or characteristics have not been removed.
   d) The subscriber's geolocation information.

3) Adds the following to the list of exemptions to the prohibition on sharing a subscriber's CPNI:
   a) Information needed to deliver wireless service to the subscriber
   b) Information needed to enact a customer-requested change in a subscriber's service.

c) Pursuant to local government subpoenas and audits to collect taxes, fees, and other charges.

4) Authorizes a telephone corporation to share a subscriber's CPNI information with its agents and affiliates to market communications services to the subscriber if the corporation obtains express written consent or federal opt-out approval.

5) Makes various definitions for the purpose of the bill, including the following:

a) CPNI means called numbers; frequency, duration, and times of calls; any services purchased by the subscriber; and other information defined as CPNI by the Federal Communications Commission (FCC).
b) Federal opt-out approval means an FCC-adopted process of in which telecommunications service provide notifies a subscriber that the subscriber's CPNI may be shared with other parties and provides the subscriber with a minimum 30-day period of time in which the subscriber can elect to opt-out before CPNI is shared.
c) Geolocation information means information used to identify the subscriber's location or the location of the subscriber's wireless device, regardless of which technology is used in the identification process.

Background

The Bounty Hunting Issue. Wireless carriers have the capacity to obtain real-time data about the location of a subscriber's wireless device by accessing a phone's global positioning system (GPS) coordinates (if available) and through pinging a phone from a nearby cell tower. Information obtained by using cell tower infrastructure to locate a specific subscriber's phone is also known as cell site location information (CSLI). Carriers can have legitimate reasons for maintaining contracts with third parties to offer geolocation services. For example, a carrier may have a contract to provide geolocation services to a company that provides automotive repair and assistance in the event that a customer's vehicle is disabled in a location where an address isn't readily available. Unlike GPS coordinates, CSLI data provides slightly less precise information that can identify the approximate location of an individual. However, this information is still considered highly sensitive and can pose a danger to a subscriber's privacy and safety if disclosed without consent and appropriate protections.

Between 2018 and 2019, several news reports revealed that websites offered to provide the real-time location of an individual's wireless device for a fee. Reports indicate that these online bounty hunters obtained real-time geolocation data

through aggregators and data brokers that either had contracts with wireless telecommunications companies or subcontracts with those companies primary aggregators. Some bounty hunters were able to obtain location data through phones' GPS and carriers' cell-tower pings. The Federal Communications Commission (FCC) is investigating the carriers' disclosure of geolocation data; however, the status of the investigation is unclear. In May 2019, the carriers reported to FCC Commissioners that they had terminated most of their agreements with third-party companies that were facilitating the sale of subscribers' geolocation data.

Federal CPNI rules. The FCC has established rules limiting telecommunications providers' ability to disclose and sell subscribers personal information. These rules are known as CPNI restrictions. However, not all data are clearly covered by these rules, and the process for obtaining a customers' consent for disclosure is not strictly with the express consent of the consumer. For example, the FCC's CPNI rules strictly prohibits the disclosure of some personal data without express consent; however, other data may be shared with the telecommunications providers' affiliates unless the customer affirmatively opts-out of CPNI disclosure. Additionally, the FCC does not require all agreements regarding CPNI disclosure to be in writing; the FCC's guidance on subscriber approval for disclosure of CPNI permits both opt-in and opt-out options for obtaining consent and under certain circumstances, the guidance permits a carrier to obtain consent to disclose CPNI orally.

This bill would codify provisions of the FCC's CPNI restrictions, and it also permits both an opt-in and opt-out framework; however, this bill also expressly includes geolocation information in the definition of CPNI. Federal statutes imply that the location of the telecommunications service is included in CPNI; however, CSLI is not expressly listed as CPNI. In a 2013 decision, the FCC determined that a wireless customer's location at the time of a call is CPNI and generally, the FCC has ruled that subscriber information is sensitive information; however, the FCC did not specify that geolocation obtained outside of a call is CPNI.

Intersection of advanced telecommunications and privacy rights. While telecommunications technology has changed significantly, existing statutes governing telecommunications subscribers' privacy rights have not been commensurately updated. Consequently, the application of privacy rights to advanced telecommunications has relied on court interpretations. However, court opinions have largely focused on the specific facts of a case and have not resolved additional ambiguities that can impact consumers. In *Carpenter v. United States*, the United States Supreme Court held that historical CSLI queries constituted a search under the 4th Amendment and require a warrant; however, the court did not

opine on real-time CSLI, and the court's evaluation of historical data was subject to the wireless carriers' retention policies. Generally, the wireless carriers maintain this information for up to five years.

For IP-based telecommunications, the lack of updated statutes and oversight of these technologies has led to some privacy implications. In a recent San Francisco Superior Court ruling for *Gruber v. Yelp*, the court determined that the California Invasion of Privacy Act (CIPA) does not apply to Voice over Internet Protocol (VoIP) calls, limiting privacy protections for calls from VoIP lines. The court determined that the Legislature had not made it clear that CIPA expressly applied to VoIP because it did not list VoIP as a covered technology in the statute and the Legislature has strictly limited the ability to regulate VoIP in the same manner as wireline telephone service. CIPA has not been updated to reflect that most consumers now use IP-based telecommunications as their primary form of telephone service.

Need for amendments. As currently written, this bill establishes prohibitions on consumer information sharing by codifying portions of the FCC's CPNI rules into state statute. However, these regulations may not be fully complementary of California privacy laws. Federal CPNI rules do not clearly establish a requirement to obtain clear consent prior to disclosure because the rules govern a wide variety of information and do not necessarily expressly encompass CSLI. California law already contains provisions establishing a telecommunications customer right to privacy. Generally, these right to privacy provisions require express consent on the customer's behalf prior to the disclosure of personal information. However, these code sections have not been fully updated to reflect current communications trends. *As a result, the author and the committee may wish to amend this bill to focus on prohibiting the sharing of CSLI within the existing laws governing wireless subscribers' right to privacy*.

Dual referral. Should this bill be approved by this committee, it will be re-referred to the Senate Committee on Judiciary for their consideration.

Prior/Related Legislation

AB 3011 (Huffman, 2008) would have expanded CPNI protections from only residential land-lines to also include mobile phones, and provided for conforming definitions and exemptions with federal law relating to CPNI. The bill died in the Assembly.

SB 697 (Hertzberg, Chapter 162, Statutes of 2015) removed a requirement to report on the helpfulness of allowing for lifeline customers disclosure for outreach purposes.

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

SUPPORT:

Consumer Reports
Media Alliance
Oakland Privacy
Public Advocates Office (formerly Office of Ratepayer Advocates)

OPPOSITION:

AT&T
CTIA
Sprint
T-Mobile
TracFone
Verizon

ARGUMENTS IN SUPPORT: According to the author:

> The sale of your mobile phone's geo-location is a fundamental violation of a subscriber's privacy. Law enforcement must obtain a warrant under both state and federal law to access your geo-location from a telecommunications provider, an appropriate safeguard that recognizances the sensitive nature of a person's current and past location. The real-world implications for personal safety are frightening when this information is shared with non-law enforcement. We must provide Californians with the tools to protect themselves, especially as the Federal Communications Commission fails to enforce federal protections

ARGUMENTS IN OPPOSITION: Opponents argue that the California Consumer Privacy Act (CCPA) already provides sufficient data protections for geolocation information and that additional requirements would result in consumer confusion. Opponents also claim that overlapping state and federal CPNI requirements would also create confusion. Opponents suggest that this bill should limit the degree to which it would require express consent from a consumer prior to any disclosure of CPNI. In opposition, CTIA states: "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."

-- END --