Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1699 (Levine) – As Amended April 22, 2019

SUBJECT: Telecommunications: public safety customer accounts: states of emergency

SUMMARY: This bill would prohibit, among other things, a mobile internet service provider (ISP) from impairing or degrading the lawful internet traffic of its public safety customer accounts, subject to reasonable network management, as specified, during a state of emergency declared by the President or the Governor, or upon the declaration of a local emergency by an official, board, or other governing body vested with authority to make such a declaration in any city, county, or city and county. This bill would state that the Legislature finds and declares that this bill is adopted pursuant to the police power granted to the State of California under the United States Constitution and cannot be preempted by the Federal Communications Commission (FCC), and that the bill ensures police and emergency services personnel have access to all of the resources necessary for them to operate effectively during a state of emergency.

EXISTING LAW:

1) Declares it unlawful for a fixed or mobile ISP, insofar as the provider is engaged in providing fixed broadband internet access service, to engage in certain activities, including, among other things:

    - Blocking lawful content, applications, services, or nonharmful devices, subject to reasonable network management.

    - Impairing or degrading lawful internet traffic on the basis of internet content, application, or service, or use of a nonharmful device, subject to reasonable network management.

    - Unreasonably interfering with, or unreasonably disadvantaging, either an end user's ability to select, access, and use broadband internet access service or the lawful internet content, applications, services, or devices of the end user's choice, or an edge provider's ability to make lawful content, applications, services, or devices available to end users, subject to reasonable network management. (Civ. Code Sec. 3101.)

2) Defines various terms for these purposes, including:

    - "Mobile ISP provides mobile broadband internet access service to an individual, corporation, government, or other customer in California.

    - "End user" to mean any individual or entity that uses a broadband internet access service.

    - "Broadband internet access service" to generally mean a mass-market retail service by wire or radio provided to customers in California that provides the capability to transmit data to, and receive data from, all or substantially all internet endpoints, including, but

not limited to, any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service.

- "Mass market" service generally means a service marketed and sold on a standardized basis to residential customers, small businesses, and other customers, including, but not limited to, schools, institutions of higher learning, and libraries. "Mass market" service does not include "enterprise service offerings" (offerings to larger organizations through customized or individually negotiated arrangements or special access services).

- "Reasonable network management" means a network management practice that is reasonable. A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for, and tailored to, achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband internet access service, and is as application-agnostic as possible. (Civ. Code Sec. 3100.)

3) Establishes within the California Office of Emergency Services (Cal OES), the Public Safety Communications Division (PSCD) to, among other things:

   - Assess the overall long-range public safety communications needs and requirements of the state considering emergency operations, performance, cost, state-of-the-art technology, multiuser availability, security, reliability, and other factors deemed to be important to state needs and requirements.

   - Develop strategic and tactical policies and plans for public safety communications with consideration for the systems and requirements of the state and all public agencies in this state, and preparing an annual strategic communications plan that includes the feasibility of interfaces with federal and other state telecommunications networks and services.

   - Providing advice and assistance in the selection of communications equipment to ensure that the public safety communications needs of state agencies are met and that procurements are compatible throughout state agencies and are consistent with the state's strategic and tactical plans for public safety communications. (Gov. Code Secs. 15277 and 15281.)

4) Provides that Cal OES shall be responsible for the state's emergency and disaster response services for natural, technological, or manmade disasters and emergencies, including responsibility for activities necessary to prevent, respond to, recover from, and mitigate the effects of emergencies and disasters to people and property. (Gov. Code Sec. 8585.) Specifies that the director of Cal OES must coordinate all state disaster response, emergency planning, emergency preparedness, disaster recovery, disaster mitigation, and homeland security activities. (Gov. Code Sec. 8585.1.) Requires Cal OES to take all necessary actions to maximize the efficiency of the "911" system. (Gov. Code Sec. 8592.9.)

5) Empowers the Governor to declare a "state of emergency" in an area affected or likely to be affected thereby when: they find that certain circumstances exist, as described below; and eitherL (1) he is requested to do so in the by a city's mayor or chief executive, or requested to do so by a county's chairman of the board of supervisors or the county administrative

officer; or, (2) he finds that local authority is inadequate to cope with an emergency. (Gov. Code Sec. 8625.)

6) Defines a "state of emergency" to mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the state caused by such conditions as air pollution, fire, flood, storm, epidemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, other than conditions resulting from a labor controversy or conditions causing a "state of war emergency," which, by reason of their magnitude, are or are likely to be beyond the control of the services, personnel, equipment, and facilities of any single county, city and county, or city and require the combined forces of a mutual aid region or regions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the California Public Utilities Commission (CPUC). (Gov. Code Sec. 8558(b).)

7) Specifies that a local emergency may be proclaimed only by the governing body of a city, county, or city and county, or by an official designated by ordinance adopted by that governing body. Defines "local emergency" to have largely the same meaning as "state emergency" but within the context of a locality, as opposed to the state. (Gov. Code Sec. 8558(c).)

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

COMMENTS:

1) **Purpose of this bill**: This bill seeks to prevent inadequate telecommunications services by impairing or degrading the lawful internet traffic of its public safety customer accounts during emergencies, as specified. This is an author-sponsored bill.

2) **Author's statement**: According to the author:

> During a declared state of emergency, public safety personnel utilize the statewide mutual aid system whereby officials can request additional aid. The effective deployment of the mutual aid system requires a high degree of coordination and real-time updates via specialized communications equipment that operates through telecommunications services.
>
> In 2018, the Mendocino Complex Fire, then the largest wildfire complex in state history, burned over 400,000 acres, destroyed 157 residences, and required deployment of public safety personnel from across the state.
>
> While combatting the Mendocino Complex Fire, Santa Clara County Fire officials experienced data throttling of mutual aid communications equipment by their telecommunications provider. As noted by Anthony Bowden, the county's fire chief, "the throttling had a significant impact on our ability to provide emergency services" and impeded the "ability to provide crisis-response and essential emergency services."

It is the responsibility of the state to provide public safety personnel with fully-functioning equipment and while steps have been taken by providers to negate a repeat situation, AB 1699 will ensure the data throttling of public safety communications equipment is never repeated.

3) **Net Neutrality background**: The term "net neutrality" refers to "internet openness"; the concept that the internet highways should be an open and equally available to all, and that no internet "traffic" should be given preference or prioritized over other traffic. Stated another way, net neutrality rules represent the principle that internet service providers (ISPs) should not discriminate against legal content and applications by blocking, throttling, or creating special "fast lanes" for certain content over others.

In 2015, the FCC adopted an Open Internet Order that established three "bright-line" rules banning these specific practices, as follows:

- No Blocking: A person engaged in the provision of broadband internet access service (BIAS), insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management.

- No Throttling: A person engaged in the provision of BIAS, insofar as such person is so engaged, shall not impair or degrade lawful Internet traffic on the basis of internet content, application, or service, or use of a non-harmful device, subject to reasonable network management.

- No Paid Prioritization: A person engaged in the provision of BIAS, insofar as such person is so engaged, shall not engage in paid prioritization. "Paid prioritization" refers to the management of a broadband provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either (a) in exchange for consideration (monetary or otherwise) from a third party, or (b) to benefit an affiliated entity. (FCC, Report and Order on Remand, Declaratory Ruling, and Order, *Protecting and Promoting the Open Internet* (Mar. 12, 2015) GN Docket No. 14-28, FCC 15-24, pp. 7-8 <https://docs.fcc.gov/public/attachments/FCC-15-24A1_Rcd.pdf> [as of Apr. 21, 2019], (hereinafter "2015 Open Internet Order").)

The FCC also adopted a catch-all standard, in addition to these three bright line rules, to prevent against negligent "mischief." Specifically, it adopted a "no unreasonable interference/disadvantage" standard prohibiting any person engaged in the provision BIAS, insofar as such person is so engaged, from unreasonably interfering with or unreasonably disadvantaging (i) end users' ability to select, access, and use BIAS or the lawful internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management, the FCC clarified, shall not be considered a violation of this rule. (*Id*.)

Ultimately, on December 14, 2017, the FCC, under the new leadership of the Trump administration, repealed the Obama-era net neutrality protections in the 2015 Open Internet Order and preempted any conflicting state laws. This put ISPs and technology companies back on the same national regulatory playing field as they were *before* 2015: the Federal

Trade Commission (FTC). Effectively, the repeal removed FCC restrictions on blocking, throttling, and prioritization, as long as such practices are publicly disclosed.

Of relevance to this bill, while throttling often is understood in the context of net neutrality discussions as the impairing or degrading of otherwise lawful internet traffic based on content or applications, the term has also been used with respect to how ISPs can slow down bandwidth or the speed available over an internet connection. As described in a more recent article:

> Very simply, bandwidth throttling means limiting how fast you can access something when online.
>
> Companies along the path between you and your web-based destination, on the other hand, often have much to gain from bandwidth throttling.
>
> For example, an ISP might throttle bandwidth during certain times of the day to decrease congestion over their network, which lowers the amount of data they have to process at once, saving them the need to buy more and faster equipment to handle internet traffic at that level.
>
> Another reason a service provider might throttle bandwidth is to provide a way for users to avoid the throttling by paying for a more expensive service that doesn't limit bandwidth. In other words, the bandwidth throttling might just be an incentive to encourage heavy users to upgrade their plan. (Fisher, *What is Bandwidth Throttling*, Lifewire <https://www.lifewire.com/what-is-bandwidth-throttling-2625808> [as of Apr. 21, 2019].)

Staff notes that this bill was recently amended, however, to remove reference to "throttling" and, instead, prohibit a mobile ISP from impairing or degrading the lawful internet traffic of its public safety customer accounts, subject to reasonable network management, during a state of emergency declared by the President or the Governor, or upon the declaration of a local emergency by an official, board, or other governing body vested with authority to make such a declaration in any city, county, or city and county. This bill relies on the definitions of "mobile ISP" and "reasonable network management" that the Legislature approved last year in passing the California Internet Consumer Protection and Net Neutrality Act of 2018.

4) **Last year's net neutrality bill does not apply to many public entity contracts but recent cases highlight the impact of throttling public safety entities' data on emergency response**: Last year, the California Internet Consumer Protection and Net Neutrality Act of 2018 was enacted by way of SB 822 (Wiener and De León, Ch. 976, Stats. 2018) to make it unlawful for an ISP, insofar as the provider is engaged in providing BIAS, to engage in certain activities, including:

   - Blocking lawful content, applications, services, or non-harmful devices, subject to reasonable network management practices.

   - Impairing or degrading lawful internet traffic on the basis of internet content, application, or service, or use of a non-harmful device, subject to reasonable network management practices.

- Unreasonably interfering with, or unreasonably disadvantaging, either an end user's ability to select, access, and use BIAS or the lawful internet content, applications, services, or devices of their choice, or an edge provider's ability to make lawful content, applications, services, or devices available to end users. Reasonable network management, as defined, would not be considered a violation of this provision.

Based on various definitions under that bill, public entities by and large do not share in those net neutrality protections. A separate bill, SB 460 (De León and Wiener) would have generally required an ISP that contracts with a state agency for any contract in the amount of $100,000 or more for the provision of BIAS to certify that it is in full compliance with, and renders BIAS to the state agency consistent with SB 822's provisions governing internet traffic, as provided. That bill ultimately failed passage on the Assembly Floor.

Since then, there have been numerous reports regarding the impact of throttling practices in public safety emergencies. In August 2018, the Sacramento Bee reported, for example:

> A Bay Area firefighting agency, assisting with the response to the massive Mendocino Complex Fire, says its communications were crippled by Verizon through a controversial practice known as "throttling."
>
> The Santa Clara County Central Fire Protection District says a communications vehicle it dispatched to the Mendocino Complex, the largest wildfire in California's history, was rendered essentially useless after Verizon reduced data speeds to a fraction of what firefighters needed.
>
> Santa Clara's complaint was lodged in a legal brief filed Monday as part of a major lawsuit aimed at restoring "net neutrality," the doctrine that says all internet traffic must be treated equally. […] Anthony Bowden, the Santa Clara fire chief, said in the court filing that its communications unit, a specially equipped recreational vehicle known as OES 5262, found its data speeds dramatically reduced when it arrived to help with the Mendocino fire, hampering communications. The issue came to a head at the end of July, as the fire was menacing areas of Mendocino and Lake counties. […]
>
> The chief said his agency complained to Verizon, but the telecom provider said the Santa Clara fire district had to switch to a more expensive data plan that would prevent throttling. Santa Clara's firefighters on the scene used other agencies' internet connections and their personal phones until the agency eventually subscribed to the better plan, he wrote. (Kasler, *Firefighters say Verizon 'throttled' data, crippling communications during California wildfire* (Aug. 22, 2018) Sacramento Bee <https://www.sacbee.com/latest-news/article217133835.html> [as of Apr. 21, 2019].)

As reported in the New York Times:

> As the largest fire on record in California continued to carve its destructive path through the northern part of the state, firefighters sent a mobile command center to the scene. With thousands of personnel, multiple aircraft and hundreds of fire engines battling the blaze, officials needed the "incident support unit" to help them track and organize all those resources.

> But in the midst of the response efforts, fire officials discovered a problem: The data connection for their support unit had been slowed to about one two-hundredth of the speed it had previously enjoyed. Like a teenager who streamed too many YouTube videos and pushed his family's usage above the limits of its data plan, the Santa Clara County Central Fire Protection District was being throttled by its internet service provider, Verizon. But in this case, officials have emphasized, homes and even lives were at stake. […]
>
> "In light of our experience, County Fire believes it is likely that Verizon will continue to use the exigent nature of public safety emergencies and catastrophic events to coerce public agencies into higher-cost plans ultimately paying significantly more for mission critical service — even if that means risking harm to public safety during negotiations," Chief Anthony Bowden said in a sworn declaration.
>
> […] In a statement on Tuesday, Verizon said it had "made a mistake in how we communicated with our customer about the terms of its plan." (Stevens, *Verizon Throttled California Firefighters' Internet Speeds Amid Blaze (They Were Out of Data)*, (Aug. 22, 2018) New York Times < https://www.nytimes.com/2018/08/22/us/verizon-throttling-california-fire-net-neutrality.html> [as of Apr. 21, 2019].)

This bill seeks prohibit any such future mistakes by expressly prohibiting a mobile ISP impairing or degrading the lawful internet traffic of its public safety customers during a state of emergency, or upon the declaration of a local emergency, as specified. In such an instance, response teams would not have to call their mobile ISP to request a lifting of their data limits; it would be incumbent upon the provider to ensure that adequate and necessary service is provided.

The California Professional Firefighters wrote in support of the introduced version of the bill:

> Nowhere is effective, timely and stable communication more critical than in the area of public safety and emergency response. Whether it's real-time medical response information or connecting the vast expanse of a massive wildfire, firefighters need to communicate quickly because every second counts.
>
> An essential component of emergency communication in the modern fire service is transmission and receipt of data. [...] Throttling data service can be disastrous to the public's safety. Indeed, an internet service provider's manipulation, or "throttling," of the data rates can render a fire department's needed communication resources virtually useless during an emergency. It can hamper radio communication among firefighters on the ground battling the blaze and impact their ability to get important safety information into the community. Additionally, throttling can impact the Reverse 9-1-1 system, which is an integral part of any emergency notification system when attempting to notify residents about imminent threats to their health and safety.
>
> California's "new normal" of wildland fires highlights the risks of physical injury faced by firefighters when battling massive fires in often unpredictable and uncontrollable conditions. At a time when firefighters are attempting to save lives and property, they cannot afford the added danger – to the safety of the public as well as their own safety –

of unnecessary interferences in the technology they rely on to do their jobs and keep civilians and themselves safe.

5) **Statement in findings and declarations regarding federal preemption**: Staff notes that the legislative findings and declarations in Section 1 of the bill state that the Legislature finds and declares that this proposed law is adopted pursuant to the police power granted to the State of California under the U.S. Constitution and cannot be preempted by the FCC. Arguably, the question of whether or not a state law is preempted is ultimately determined by the Supremacy Clause of the federal Constitution, as interpreted by the courts in the context of a state law that conflicts with federal law, either expressly or impliedly. (*See* U.S. Const., art. VI.) Additionally, if the federal government passes a law specific to this issue under its authorities granted by the Constitution, they may choose to expressly preempt this and other state laws in part or in whole under that same clause – which the State cannot preclude, again, as a matter of the Supremacy Clause. To declare that this bill cannot be preempted, even as uncodified findings and declarations, suggests that the Legislature has authority to limit the federal government's authority, or pre-determine the judicial branch's interpretations of the law, when it does not. Accordingly, the author may wish to either restate the intent with respect to preemption, or strike it from the bill.

6) **Other arguments in support**: In support of the introduced version of this bill, EFF wrote:

> […] Verizon's throttling of public safety had nothing to do with engineering or any justification that would come close to resembling reasonable network management. Rather, what befell public safety entities was a business practice of arbitrarily establishing a data cap that renders a service useless in order to incentivize a paying customer to purchase a more expensive plan. However, Santa Clara County stated to the D.C. Circuit in its affidavit that it was represented to them that Verizon was selling them a fully unlimited plan without restraints. In the aftermath, Verizon has issued an apology and admitted fully to the error.
>
> The events in Santa Clara, where fire fighters had their wireless data plans throttled to essentially being unusable in the middle of a state emergency, should never be repeated. The conduct of Verizon, were the 2015 Open Internet Order still in effect, likely violated the federal ban on unjust and unreasonable conduct, and in the absence AB 1699, no state or federal laws in effect squarely address the situation.

Also in support of the introduced version of this bill, the California Central Valley Flood Control Association (CCVFCA) wrote in support to the introduced version of the bill:

> The California Public Utilities Commission (CPUC) has regulatory authority over telephone corporations. […] According to the CPUC, "California needs a resilient, reliable and effective system of communicating with first responders, local and state governments and the public when disasters strike. And the truth is, we do not have that system today." The director of the Los Angeles County Office of Emergency Management has drawn attention to the questionable resiliency of the communications grid as one of his top safety concerns. He has also observed that cellular providers are not as integrated or immersed into the emergency management community as other utility providers. AB 1699 could help ensure that an adequate level of telecommunications services is provided for public safety customer accounts during an emergency. However,

the Legislature and CPUC must address the larger issue of the resiliency of the communications grid under various disaster scenarios; e.g., wildfire, earthquake and flood. While prohibiting the throttling of accounts would benefit first responders, the potential loss of cell towers and the lack of backup electric power for cell towers and IP services must be addressed going forward.

7) **CTIA request for amendments**: In an "oppose unless amended" letter tailored to the introduced version of this bill, CTIA argued that: (1) the bill's do "not impair or degrade" standard is ambiguous and may result in serious unintended consequences, including needless litigation; (2) the bill's "emergency" trigger is excessive and should be limited to a "state of emergency" declared by the President or the Governor; (3) the bill should include notification requirements to service providers; and, (4) the bill is misplaced within the Public Utilities Code. Specifically, CTIA argued the following:

   - Data prioritization for first responders is already provided by major mobile wireless providers and wireless carriers need the flexibility to manage their network traffic for optimum performance, especially during disasters. The vague terms of "impair or degrade" may result in serious unintended consequences and could invite litigation.

   - Using a declared 'state of emergency' – particularly at the local level - as the trigger for the obligations not to impair or degrade is problematic from an operational perspective. How would carriers learn of the emergency declaration in small county X or little town Y in a timely manner? How would carriers adjust their practices or service features to accommodate the emergency only in a small, specific geographic area? How could carriers account for and treat public safety customers and non-local public safety customers responding to that emergency from other jurisdictions?

   - The bill should require the authorities declaring an emergency to notify service providers of any such declaration and the scope of the emergency. Additionally, the holder of the affected public safety account should be required to notify the carrier regarding the declared state of emergency as is the case today. Data prioritization for first responders during emergencies is already provided by major mobile wireless providers. Allowing public safety to self-identify and request relief from their carrier is simpler and more effective than forcing a carrier to proactively try to determine which accounts belong to public safety customers and whether any service adjustments are necessary due to an emergency situation.

   - The Office of Emergency Services (OES) is the appropriate entity to deal with issues related to emergencies. (Subheadings omitted.)

8) **Prior legislation**: AB 822 (Wiener and De León, Ch. 976, Stats. 2018) *See* Comment 4.

   SB 460 (De León and Wiener, 2018) *See* Comment 4.

9) **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 12-0 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

California Central Valley Flood Control Association
California Fire Chiefs Association
California Professional Firefighters
County of Santa Clara
Electronic Frontier Foundation
Fire Districts Association of California
Public Advocates Office

Opposition

CTIA – The Wireless Association (unless amended)

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