

EXHIBIT TURN-X-30

Assembly Bill No. 1699

CHAPTER 398

An act to add Section 2898 to the Public Utilities Code, relating to telecommunications.

[Approved by Governor October 2, 2019. Filed with Secretary
of State October 2, 2019.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1699, Levine. Telecommunications: mobile internet service providers: first response agencies: emergencies.

Existing law prohibits a mobile internet service provider from engaging in specified actions concerning the treatment of internet traffic, including, among other things, blocking lawful content, applications, services, or nonharmful devices, and 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.

This bill would authorize a first response agency to submit a request to a mobile internet service provider to not impair or degrade the lawful internet traffic of an account used by the agency in response to an emergency, and would require a first response agency that acts pursuant to that authorization to notify the mobile internet service provider upon the account no longer being used by the agency in response to the emergency. The bill would prohibit the mobile internet service provider, upon receiving that request, from impairing or degrading the lawful internet traffic of the first response agency's account until the earlier of either the time when the account is no longer being used by the agency in response to the emergency or the end of the emergency, subject to reasonable network management.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares that this act is adopted pursuant to the police power granted to the State of California. This act is adopted to protect and promote the safety, life, public health, public convenience, general prosperity, and well-being of society, and the welfare of the state's population and economy. This act ensures police and emergency services personnel have access to all of the resources necessary for them to operate effectively during an emergency.

SEC. 2. Section 2898 is added to the Public Utilities Code, to read:

2898. (a) Notwithstanding any other provision of this part, upon receiving a request pursuant to subdivision (b), the mobile internet service provider shall not impair or degrade the lawful internet traffic of the first

Ch. 398

— 2 —

response agency's identified account until the earlier of either the account no longer being used by the agency in response to the emergency or the end of the emergency, subject to reasonable network management.

(b) (1) A first response agency may submit a request to a mobile internet service provider to not impair or degrade the lawful internet traffic of an account used by the agency in response to an emergency. As part of the request, the first response agency shall identify the account number and lines for the mobile internet service provider.

(2) A first response agency that submits a request pursuant to paragraph (1) shall notify the mobile internet service provider upon the account no longer being used by the agency in response to the emergency.

(c) For purposes of this section, the following definitions apply:

(1) "Emergency" means the existence of conditions of disaster or of extreme peril to the safety of persons and property within the state, or the territorial limits of a county, city and county, or city, caused by a fire, flood, storm, riot, cyberterrorism, sudden and severe energy shortage, Governor's warning of an earthquake or volcanic prediction, earthquake, or other similar condition.

(2) "First response agencies" has the same meaning as defined in Section 8592.1 of the Government Code, and shall include fire districts.

(3) "Mobile internet service provider" has the same meaning as defined in Section 3100 of the Civil Code.

(4) "Reasonable network management" has the same meaning as defined in Section 3100 of the Civil Code.

Date of Hearing: April 24, 2019

ASSEMBLY COMMITTEE ON COMMUNICATIONS AND CONVEYANCE

Miguel Santiago, Chair

AB 1699 (Levine) – As Amended April 22, 2019

SUBJECT: Telecommunications: mobile internet service providers: public safety customer accounts: states of emergency.

SUMMARY: Prohibits a mobile internet service provider 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 of the United States 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.

EXISTING LAW:

- 1) Specifies that the Governor is empowered to proclaim a state of emergency in an area affected or likely to be affected thereby when:
 - a) He finds that specified circumstances exist;
 - b) He is requested to do so in the case of a city by the mayor or chief executive, in the case of a county by the chairman of the board of supervisors or the county administrative officer; or,
 - c) He finds that local authority is inadequate to cope with the emergency. (Government Code (GOV) Section 8625)
- 2) 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 Section 8558 (b))
- 3) 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. (GOV Section 8630)
- 4) Defines a “Local emergency” to mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the territorial limits of a county, city and county, or city, caused by conditions such as air pollution, fire, flood, storm,

epidemic, riot, drought, cyberterrorism, 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, which are or are likely to be beyond the control of the services, personnel, equipment, and facilities of that political subdivision and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the CPUC. (GOV Section 8558 (c))

- 5) Makes it unlawful for a fixed or mobile internet service provider (ISP), insofar as the provider is engaged in providing broadband Internet access service, to engage in the specified activities that interferes with a users' ability to access content on the internet. (Civil Code Section 3100 et seq.)

FISCAL EFFECT: Unknown. This bill has been keyed non-fiscal by the Legislative Counsel.

COMMENTS:

- 1) **Authors Statement:** According to the author, "While combatting the Mendocino Complex Fire, Santa Clara County Fire officials experienced data throttling of mutual aid communications equipment by their telecommunications service provider, Verizon Wireless [...] 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."
- 2) **Background:** Although California is no stranger to natural disasters, the scale and frequency of recent wildfires has pose a continuous threat to public health and safety. California's fire season normally peaks in October, but due to the combination of strong winds, low humidity, and climate change, 2017 and 2018 saw a series of wildfires that broke previous wildfire records across the State. In December 2017, the Thomas Fire became the largest wildfire in California history. But by July 2018, that record had been eclipsed by the Mendocino Complex Fires, which burned more than 459,000 acres across four counties. A month later, the Camp Fire broke out in the foothills of Butte County. By the time the Camp Fire was fully contained over 19,000 properties had been destroyed, 85 residents were killed with hundreds more homeless and unaccounted for, and the town of Paradise was completely destroyed.
- 3) **Emergency Declarations:** Governors are tasked with ensuring that their state is adequately prepared for emergencies and disasters. While most day to day emergency situations such as fires, power outages, hazardous material spills, are handled at the local level, some raise to the level of requiring a response beyond the capacity of local governments or even the state. Current law empowers the Governor to proclaim a state of emergency in an area affected by certain circumstances such as fires, floods, earthquakes, epidemics, riots, and drought. Governors may also declare a state of emergency if they are requested to do so by local executives such as a mayor or the chair of the county board of supervisors, or if they find that the local authority is inadequate to cope with the emergency. Local governments can declare local emergencies if a disaster or emergency affects the territorial limits of its jurisdiction, but may not rise to the state level.

- 4) **Mendocino Complex Fire:** The Mendocino Complex Fire comprised of two wildfires, the River Fire and the Ranch Fire that broke out on July 27, 2018, burning in Mendocino, Lake, Colusa, and Glenn County. The River Fire was contained on August 13th while the Ranch Fire was not contained until September 18th. By the time the Mendocino Complex Fire was contained it was the biggest complex fire; with the Ranch Fire by itself being the largest single wildfire, in California history. The Mendocino Complex Fire burned over 459,000 acres and destroyed over 500 buildings.
- 5) **Verizon Throttling during Mendocino Fires:** During the Mendocino Complex Fire, the Santa Clara Fire Department, which had been deployed to provide mutual aid, began experiencing a dramatic decrease in the data connection speed of their communications equipment to the point where it severely interfered with the Department's ability to function effectively. The Santa Clara Fire Department contacted its ISP, Verizon, which explained that the Department's service plan, while offering unlimited data, had a provision in which its data speed would decrease considerably once a certain threshold of data had been exceeded in a given billing cycle. The Department asked Verizon to end the throttling in light of the emergency situation, however, it only ended after the Department agreed to purchase another plan that included a higher data threshold. Following the incident, Verizon acknowledged that it had made a mistake and issued an apology in which it stated,

"In supporting first responders in the Mendocino fire, we didn't live up to our own promise of service and performance excellence when our process failed some first responders on the line, battling a massive California wildfire. For that, we are truly sorry. And we're making every effort to ensure that it will never happen again."

This bill prohibits a mobile internet service provider from impairing or degrading the lawful internet traffic of its public safety customer accounts during an emergency. Needless to say, the throttling of our first responder emergency communication networks can have a dramatic impact on their ability to protect public safety and save lives. The events of 9/11 for example, demonstrated how the failure of our first responder's communications network during a crisis led to confusion and delays in rescue operations and coordination.

- 6) **Net Neutrality?** Net neutrality is the principle that ISPs should not discriminate against legal content and applications, by charging edge providers different delivery speed to deliver their content. Hence ISPs should not block, throttle, or create special "fast lanes" for certain content. Following the Mendocino Complex Fire incident, the Santa Clara Fire Chief submitted a declaration supporting a petition seeking to restore net neutrality rules that the Federal Communications Commission had repealed.

Although some have associated the act of throttling during the Mendocino Complex Fire as an example of a net neutrality violation, it is important to note that throttling in regards to net neutrality is not simply the impairing or degrading of lawful internet traffic, but the impairing or degrading lawful internet traffic *on the basis of Internet content, application, or service*. In the case of the Mendocino Complex Fire, the throttling, as far as we know, was not discriminatory based on the *content* that was being delivered through the network. The incident arguably was a clear failure in customer service on the part of Verizon, but it did not demonstrate a net neutrality violation.

- 7) **Arguments in Support:** According to the California Professional Firefighters, “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 [ISP’s] manipulation, or ‘throttling,’ of the data rates can render a fire department’s needed communication resources virtually useless during an emergency [...] 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.
- 8) **Arguments in Opposition:** According to CTIA, “The bill’s vague mandates, problematic emergency trigger requirement and failure to include notification requirements could work to impede activities by first responders during disasters [...] AB 1699’s ‘not impair or degrade’ standard is ambiguous and may result in serious unintended consequences, including needless litigation [...] The ‘emergency trigger’ for AB 1699 is excessive and should be limited to a ‘state of emergency’ declared by the President or the Governor [...] AB 1699 should include notification requirements [...] AB 1699’s provisions should not be in the Public Utilities Code [...] For these reasons, CTIA must oppose AB 1699 unless it is amended to address the foregoing concerns and looks forward to working with the author to that end.”
- 9) **Prior Legislation:** AB 1999 (Chau) of 2018 established net neutrality rules for local agencies that provide broadband services and expands the type of local agencies that may provide broadband infrastructure. *Status: Chaptered by the Secretary of State – Chapter 963, Statutes of 2018.*
- SB 822 (Wiener) of 2018 established net neutrality rules by prohibiting internet service providers from engaging in activities that interfere with a user’s ability to access content on the internet. *Status: Chaptered by the Secretary of State – Chapter 976, Statutes of 2018.*
- 10) **Double-referral:** This bill is double referred, and if passed by this Committee, will be referred to the Assembly Committee on Privacy and Consumer Protection.

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: Edmond Cheung / C. & C. / (916) 319-2637

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 “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

ASSEMBLY THIRD READING
AB 1699 (Levine)
As Amended April 22, 2019
Majority vote

SUMMARY:

Prohibits 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, during a state of emergency declared by the President of the United States 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.

COMMENTS:

Verizon Throttling during Mendocino Fires: During the 2018 Mendocino Complex Fire, the Santa Clara Fire Department experienced a dramatic decrease in the data connection speed of their communications equipment to the point where it severely interfered with the Department's ability to function effectively. The Department contacted its ISP, Verizon, which told them that their service plan, while offering unlimited data, had a provision in which its data speed would decrease considerably once a certain threshold of data had been exceeded in a given billing cycle. The Department asked Verizon to end the throttling in light of the emergency situation, however, it only ended after the Department agreed to purchase another plan that included a higher data threshold. Following the incident, Verizon acknowledged that it had made a mistake and issued an apology.

According to the Author:

While combatting the Mendocino Complex Fire, Santa Clara County Fire officials experienced data throttling of mutual aid communications equipment by their telecommunications service provider, Verizon Wireless [...] 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, this bill will ensure the data throttling of public safety communications equipment is never repeated.

Arguments in Support:

According to the California Professional Firefighters, "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 [ISP's] manipulation, or 'throttling' of the data rates can render a fire department's needed communication resources virtually useless during an emergency [...] 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."

Arguments in Opposition:

According to CTIA, "The bill's vague mandates, problematic emergency trigger requirement and failure to include notification requirements could work to impede activities by first responders during disasters [...] AB 1699's 'not impair or degrade' standard is ambiguous and may result in serious unintended consequences, including needless litigation [...] The 'emergency trigger' for AB 1699 is excessive and should be limited to a 'state of emergency' declared by the President or

the Governor [...] AB 1699 should include notification requirements [...] AB 1699's provisions should not be in the Public Utilities Code [...] For these reasons, CTIA must oppose AB 1699 unless it is amended to address the foregoing concerns and looks forward to working with the author to that end."

FISCAL COMMENTS:

Unknown. This bill has been keyed non-fiscal by the Legislative Counsel.

VOTES:

ASM COMMUNICATIONS AND CONVEYANCE: 12-0-1

YES: Santiago, Obernolte, Boerner Horvath, Bonta, Brough, Gipson, Holden, Kamlager-Dove, Low, Patterson, Quirk-Silva, Rodriguez

ABS, ABST OR NV: Cervantes

ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0

YES: Chau, Kiley, Bauer-Kahan, Berman, Calderon, Gabriel, Gallagher, Irwin, Obernolte, Smith, Wicks

UPDATED:

VERSION: April 22, 2019

CONSULTANT: Edmond Cheung / C. & C. / (916) 319-2637

FN: 0000360

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

Bill No: AB 1699 **Hearing Date:** 7/10/2019
Author: Levine
Version: 6/24/2019 As Amended
Urgency: No **Fiscal:** No
Consultant: Sarah Smith

SUBJECT: Telecommunications: mobile internet service providers: first response agencies: emergencies

DIGEST: This bill prohibits mobile internet service providers (ISPs) from impairing or degrading the lawful internet traffic of first response agencies during an emergency.

ANALYSIS:

Existing law:

- 1) Makes various definitions for the purpose of establishing net neutrality requirements, including, but not limited to, the following:
 - a) Mobile ISP is a business that provides mobile broadband internet access service to customers within California.
 - b) Reasonable network management is network management that is reasonable. A network management practice is reasonable if it primarily used for legitimate network management purposes. (Civil Code §3100)
- 2) Prohibits ISPs from engaging in certain activities that impact a consumer's ability to lawfully access content on the internet, including, but not limited to the following:
 - a) Intentionally blocking lawful content, slowing or speeding traffic, or otherwise interfering with access to lawful content on the basis of source, destination, internet content, application, or service, or use of a non-harmful device.
 - b) Engaging in third-party paid prioritization.
 - c) Selectively zero-rating some internet content, applications, services, or devices or zero-rating in exchange for consideration or payment.
 - d) Engaging in practices that have the purpose of evading net neutrality requirements. This prohibition may not be construed as prohibiting ISP traffic exchange agreements that comply with net neutrality requirements.

- e) Failing to publicly disclose accurate information about the network management practices, performance, and commercial terms of its broadband internet access services to enable consumers to make informed choices about those services.
 - f) Requiring consideration from edge providers, monetary or otherwise, for access to an ISP's end users. (Civil Code §3101)
- 3) Prohibits mobile and fixed ISPs from offering services other than broadband internet access service over last-mile connection if those other services can be used as an equivalent of broadband internet and do at least one of the following:
- a) Have the effect of evading net neutrality requirements or
 - b) Negatively impact the performance of broadband access internet services.
- (Civil Code §3102)
- 4) Specifies that nothing limits ISPs from meeting the needs of emergency communications, law enforcement, public safety, or national security authorities. (Civil Code §3103)

This bill:

- 1) Prohibits mobile ISPs from impairing or degrading the lawful internet traffic of first response agencies for at least 48 hours after receiving notification that the agency is responding to an emergency.
- 2) Prohibits mobile ISPs from impairing or degrading the lawful internet traffic of first response agencies for the duration of an emergency upon receiving notification that the agency is responding to an emergency.
- 3) Makes this bill's prohibitions on impairing or degrading lawful internet traffic subject to reasonable network management practices.
- 4) Authorizes the Director of the Office of Emergency Services (OES) or a designee to identify local agencies that will respond to an emergency and requires the Director of OES to notify the relevant mobile ISPs of the agencies responding to an emergency.
- 5) Requires OES to do the following upon identifying the local agencies that will respond to an emergency:
 - a) Notify the relevant mobile ISPs of the agencies responding to the emergency.
 - b) Provide the relevant mobile ISPs with a point of contact to provide updates about the emergency and the agencies responding to the emergency.

- 6) Makes various definitions for the purposes of this bill, including defining an emergency as a state or local emergency and specifying that mobile ISP and reasonable network management have the same meaning as those terms are used for net neutrality.

Background

California's net neutrality requirements. Last year, the Legislature passed SB 822 (Weiner, Chapter 976, Statutes of 2018), which established net neutrality requirements within California. These requirements prohibit an ISP from engaging in activities that impair or degrade end user's ability to lawfully access internet traffic. Specifically, the bill prohibits ISPs from blocking, throttling, engaging in paid prioritization, selectively zero-rating, and requiring consideration from edge providers to deliver content to end users. California's net neutrality provisions largely apply to fixed ISP connections; however, it prohibits mobile ISP from offering products that have the purpose of evading net neutrality requirements. This bill prohibits mobile ISPs from impairing or degrading a first response agency's lawful internet access while the agency is responding to an emergency.

Throttling of firefighters during Mendocino Complex Fire response. While the Legislature was considering net neutrality requirements, the Santa Clara County Fire Department (SCCFD) filed a complaint in a federal court proceeding stating that Verizon throttled the SCCFD's data while the SCCFD was dispatched to provide mutual aid during the Mendocino Complex Fire. The SCCFD deployed an OES 5262 incident command truck that uses software to conduct real-time tracking of resources responding to the fire. The truck's software relies heavily on the ability to send and receive large volumes of data when in use.

The SCCFD had a plan from Verizon that included unlimited data; however, the plan's terms permitted throttling when more than a certain volume of data is used during the monthly billing cycle. The throttling effectively limited the first responders' ability to use OES 5262 until it could resolve the data limitations. Once the SCCFD realized that its internet data speed had slowed dramatically, it contacted Verizon to remove the data limit. However, Verizon did not immediately remove the data restrictions; instead, a customer service representative informed the SCCFD that it would need to upgrade the plan that cost more than double the SCCFD's existing monthly cost to prevent throttling. The SCCFD ultimately upgraded its plan and Verizon removed the throttling. After the SCCFD's complaint became public, Verizon apologized for the error and committed to taking steps to prevent throttling of public safety accounts in the future. In an August 2018, informational hearing held by the Assembly Select Committee on Natural Disaster Response, Recovery, and Rebuilding,

representatives for Verizon discussed plans to establish a new program for public safety accounts that would not contain data limitations and would include priority data access at no additional cost.

This bill would establish a notification process for first response agencies to notify their respective ISPs of the need to lift data restrictions when responding to disasters. Under this bill, OES would be responsible for identifying the agencies that must respond to a disaster and notifying the relevant mobile ISPs of the need to remove any data limitations.

This bill may apply only when a local agency is providing mutual aid. This bill would require mobile ISPs to lift data restrictions upon receiving notification from OES that certain local agencies are responding to an emergency. Under this bill, OES would be responsible for identifying the local agencies that would need data restrictions lifted and notify the mobile ISPs of the local agencies' need to have data limitations lifted. The role of OES in notifying ISPs implies that this bill's notification process will only apply in circumstances when OES is coordinating local mutual aid because not all emergency response is coordinated through OES. A number of local emergencies may not result in an emergency declaration at the start of an emergency. For example, an active shooter incident may result in a significant local emergency response effort; however, those resources may not be coordinated through OES. To ensure that OES's notification process is streamlined, local agencies would likely need to provide OES with information about their respective mobile ISP services, including account numbers, providers and potential plan limitations.

Need for amendments. As currently drafted, this bill would require mobile ISPs to lift data restrictions for first response agencies upon receiving notice from OES that the agency is responding to an emergency. The use of OES as the primary notification agency implies that this bill would only apply to emergencies for which OES is coordinating mutual aid. As a result, local agencies may not have the ability to use this bill to lift data restrictions when responding to an emergency without OES coordination. This bill requires the ISP to lift data restrictions for both at least 48 hours and the duration of the emergency. However, it is not clear whether the ISP would be required to lift the data restrictions for at least 48 hours in the event that an emergency lasts for a shorter duration. Additionally, this bill's provisions establishing a notification process for requesting removal of data limitations for certain agencies is unclear. While this bill requires OES to notify ISPs of the agencies responding to the emergency, this notification may not identify the accounts linked to resources that are being used. This lack of clarity may increase the likelihood of miscommunications during an emergency response effort requiring mutual aid. *As a result, the author and this committee may wish to*

amend this bill to clarify the durations for which an ISP must lift data restrictions, specify that an ISP must lift data restrictions for first response agencies upon receiving notification of the accounts for which restrictions must be lifted, and allow local agencies to notify their ISPs that data restrictions must be lifted without requiring OES coordination.

Prior/Related Legislation

SB 822 (Weiner, Chapter 976, Statutes of 2018) established net neutrality requirements in California by prohibiting ISPs from taking certain actions that interfere with consumers' ability to lawfully access internet content, including impairing or degrading lawful internet traffic. The bill prohibited intentionally blocking content, speeding up or slowing down traffic, engaging in paid-prioritization, requiring consideration from edge providers for access to an ISP's end users, and selectively zero-rating certain content.

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

SUPPORT:

California Central Valley Flood Control Association
California Fire Chiefs Association
California Professional Firefighters
City of Thousand Oaks
County of Santa Clara
Electronic Frontier Foundation
Fire Districts Association of California
League of California Cities
Media Alliance
Public Advocates Office (formerly Office of Ratepayer Advocates)

OPPOSITION:

CTIA

ARGUMENTS IN SUPPORT: According to the author:

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 service provider, Verizon Wireless. 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.

ARGUMENTS IN OPPOSITION: CITA, the trade association for the wireless communications industry opposes this bill unless it is amended to remove this bill from the Public Utilities Code, clarify the public safety accounts to which this bill applies, and clarify the meaning of the term "impair or degrade" as it applies to internet traffic. In opposition, CTIA states the following:

...our concern is the AB 1699 may have unintended consequences and could actually undermine, not aid, public safety access during emergencies. As such, CTIA opposes AB 1699 as drafted, but will continue to work with the author and public safety on our mutual goals.

-- END --

SENATE RULES COMMITTEE
Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

AB 1699

THIRD READING

Bill No: AB 1699
Author: Levine (D)
Amended: 8/13/19 in Senate
Vote: 21

SENATE ENERGY, U. & C. COMMITTEE: 11-0, 7/10/19
AYES: Hueso, Moorlach, Bradford, Chang, Dodd, Hertzberg, Hill, McGuire,
Stern, Stone, Wiener
NO VOTE RECORDED: Rubio, Skinner

ASSEMBLY FLOOR: 75-0, 5/9/19 - See last page for vote

SUBJECT: Telecommunications: mobile internet service providers: first
response agencies: emergencies

SOURCE: Author

DIGEST: This bill prohibits mobile Internet service providers (ISPs) from impairing or degrading the lawful Internet traffic of first response agencies during an emergency.

ANALYSIS:

Existing law:

- 1) Makes various definitions for the purpose of establishing net neutrality requirements, including, but not limited to, the following:
 - a) Mobile ISP is a business that provides mobile broadband Internet access service to customers within California.
 - b) Reasonable network management is network management that is reasonable. A network management practice is reasonable if it primarily used for legitimate network management purposes. (Civil Code §3100)

- 2) Prohibits ISPs from engaging in certain activities that impact a consumer's ability to lawfully access content on the Internet, including, but not limited to the following:
 - a) Intentionally blocking lawful content, slowing or speeding traffic, or otherwise interfering with access to lawful content on the basis of source, destination, Internet content, application, or service, or use of a non-harmful device.
 - b) Engaging in third-party paid prioritization.
 - c) Selectively zero-rating some Internet content, applications, services, or devices or zero-rating in exchange for consideration or payment.
 - d) Engaging in practices that have the purpose of evading net neutrality requirements. This prohibition may not be construed as prohibiting ISP traffic exchange agreements that comply with net neutrality requirements.
 - e) Failing to publicly disclose accurate information about the network management practices, performance, and commercial terms of its broadband Internet access services to enable consumers to make informed choices about those services.
 - f) Requiring consideration from edge providers, monetary or otherwise, for access to an ISP's end users. (Civil Code §3101)
- 3) Prohibits mobile and fixed ISPs from offering services other than broadband Internet access service over last-mile connection if those other services can be used as an equivalent of broadband Internet and do at least one of the following:
 - a) Have the effect of evading net neutrality requirements or
 - b) Negatively impact the performance of broadband access Internet services. (Civil Code §3102)
- 4) Specifies that nothing limits ISPs from meeting the needs of emergency communications, law enforcement, public safety, or national security authorities. (Civil Code §3103)

This bill:

- 1) Prohibits mobile ISPs from impairing or degrading the lawful Internet traffic of first response agencies after receiving notification that the agency is responding to an emergency. After receiving this notification, ISPs may not impair or

degrade the traffic for at least 48 hours or for the duration of the emergency, depending on which is longer.

- 2) Makes this bill's prohibitions on impairing or degrading lawful Internet traffic subject to reasonable network management practices.
- 3) Authorizes first response agencies to request removal of data restrictions when responding to an emergency and requires these agencies to notify an ISP when the agency ceases to participate in the emergency response.
- 4) Makes various definitions for the purposes of this bill, including defining an emergency as a state or local emergency and specifying that mobile ISP and reasonable network management have the same meaning as those terms are used for net neutrality.

Background

California's net neutrality requirements. Last year, the Legislature passed SB 822 (Weiner, Chapter 976, Statutes of 2018), which established net neutrality requirements within California. These requirements prohibit an ISP from engaging in activities that impair or degrade end user's ability to lawfully access Internet traffic. Specifically, the bill prohibits ISPs from blocking, throttling, engaging in paid prioritization, selectively zero-rating, and requiring consideration from edge providers to deliver content to end users. California's net neutrality provisions largely apply to fixed ISP connections; however, it prohibits mobile ISP from offering products that have the purpose of evading net neutrality requirements. This bill prohibits mobile ISPs from impairing or degrading a first response agency's lawful Internet access while the agency is responding to an emergency.

Throttling of firefighters during Mendocino Complex Fire response. While the Legislature was considering net neutrality requirements, the Santa Clara County Fire Department (SCCFD) filed a complaint in a federal court proceeding stating that Verizon throttled the SCCFD's data while the SCCFD was dispatched to provide mutual aid during the Mendocino Complex Fire. The SCCFD deployed an OES 5262 incident command truck that uses software to conduct real-time tracking of resources responding to the fire. The truck's software relies heavily on the ability to send and receive large volumes of data when in use.

The SCCFD had a plan from Verizon that included unlimited data; however, the plan's terms permitted throttling when more than a certain volume of data is used during the monthly billing cycle. The throttling effectively limited the first responders' ability to use OES 5262 until it could resolve the data limitations.

Once the SCCFD realized that its Internet data speed had slowed dramatically, it contacted Verizon to remove the data limit. However, Verizon did not immediately remove the data restrictions; instead, a customer service representative informed the SCCFD that it would need to upgrade the plan that cost more than double the SCCFD's existing monthly cost to prevent throttling. The SCCFD ultimately upgraded its plan and Verizon removed the throttling. After the SCCFD's complaint became public, Verizon apologized for the error and committed to taking steps to prevent throttling of public safety accounts in the future. In an August 2018, informational hearing held by the Assembly Select Committee on Natural Disaster Response, Recovery, and Rebuilding, representatives for Verizon discussed plans to establish a new program for public safety accounts that would not contain data limitations and would include priority data access at no additional cost.

This bill establishes a notification process for first response agencies to notify their respective ISPs of the need to lift data restrictions when responding to disasters. Under this bill, an ISP must lift data restrictions for at least 48 hours or for the duration of the emergency, depending on which is longer. A first response agency making a request must identify the account number for which data restrictions should be removed. An agency that has made a request for removal of data restrictions must notify the ISP once the agency ceases to respond to the emergency.

States of emergency. This bill does not require a state of emergency proclamation as a prerequisite for requesting removal of data restrictions; however, it defines emergencies using definitions from existing law. These existing definitions characterize local and state emergencies as those that are duly proclaimed. Emergency proclamations frequently are not issued at the start of a local or state emergency. As a result, first response agencies may respond to an emergency for an extended duration of time before a proclamation of the emergency exists. First response agencies likely need data restrictions removed prior to the proclamation of an emergency. Local first response agencies may also cease to respond to an emergency prior to the declared end of an emergency. This bill authorizes local agencies to request the removal of data restrictions when responding to an emergency and requires the agencies making these requests to notify their respective ISPs once they cease to respond to the emergency.

Related/Prior Legislation

SB 822 (Weiner, Chapter 976, Statutes of 2018) established net neutrality requirements in California by prohibiting ISPs from taking certain actions that

interfere with consumers' ability to lawfully access Internet content, including impairing or degrading lawful Internet traffic. The bill prohibited intentionally blocking content, speeding up or slowing down traffic, engaging in paid-prioritization, requiring consideration from edge providers for access to an ISP's end users, and selectively zero-rating certain content.

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

SUPPORT: (Verified 8/13/19)

California Central Valley Flood Control Association
California Fire Chiefs Association
California Professional Firefighters
City of Thousand Oaks
County of Santa Clara
Electronic Frontier Foundation
Fire Districts Association of California
League of California Cities
Media Alliance
Public Advocates Office (formerly Office of Ratepayer Advocates)

OPPOITION: (Verified 8/13/19)

CTIA

ARGUMENTS IN SUPPORT: According to the author:

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 service provider, Verizon Wireless. 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.

ARGUMENTS IN OPPOSITION: CTIA, the trade association for the wireless communications industry opposes this bill unless it is amended to remove this bill from the Public Utilities Code, clarify the public safety accounts to which this bill applies, and clarify the meaning of the term “impair or degrade” as it applies to Internet traffic. In opposition, CTIA states the following:

...our concern is the AB 1699 may have unintended consequences and could actually undermine, not aid, public safety access during emergencies. As such, CTIA opposes AB 1699 as drafted, but will continue to work with the author and public safety on our mutual goals.

ASSEMBLY FLOOR: 75-0, 5/9/19

AYES: Aguiar-Curry, Bauer-Kahan, Berman, Bloom, Boerner Horvath, Bonta, Brough, Burke, Calderon, Carrillo, Cervantes, Chau, Chiu, Choi, Chu, Cooley, Cooper, Cunningham, Daly, Diep, Eggman, Flora, Fong, Frazier, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Gloria, Gonzalez, Gray, Grayson, Holden, Irwin, Jones-Sawyer, Kalra, Kamlager-Dove, Kiley, Lackey, Levine, Limón, Low, Maienschein, Mathis, Mayes, Medina, Melendez, Mullin, Muratsuchi, Nazarian, Obernolte, O'Donnell, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Smith, Mark Stone, Ting, Voepel, Waldron, Weber, Wicks, Wood, Rendon

NO VOTE RECORDED: Arambula, Bigelow, Chen, Dahle, McCarty

Prepared by: Sarah Smith / E., U., & C. / (916) 651-4107
8/14/19 15:20:11

**** **END** ****

SENATE RULES COMMITTEE
Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

AB 1699

THIRD READING

Bill No: AB 1699
Author: Levine (D)
Amended: 9/5/19 in Senate
Vote: 21

SENATE ENERGY, U. & C. COMMITTEE: 11-0, 7/10/19
AYES: Hueso, Moorlach, Bradford, Chang, Dodd, Hertzberg, Hill, McGuire,
Stern, Stone, Wiener
NO VOTE RECORDED: Rubio, Skinner

ASSEMBLY FLOOR: 75-0, 5/9/19 - See last page for vote

SUBJECT: Telecommunications: mobile internet service providers: first
response agencies: emergencies

SOURCE: Author

DIGEST: This bill prohibits mobile Internet service providers (ISPs) from impairing or degrading the lawful Internet traffic of first response agencies during an emergency.

Senate Floor Amendments of 9/5/19 clarify the definition of an emergency for the purposes of this bill and the process for lifting first response agencies' data restrictions.

ANALYSIS:

Existing law:

- 1) Makes various definitions for the purpose of establishing net neutrality requirements, including, but not limited to, the following:
 - a) Mobile ISP is a business that provides mobile broadband Internet access service to customers within California.

- b) Reasonable network management is network management that is reasonable. A network management practice is reasonable if it primarily used for legitimate network management purposes. (Civil Code §3100)
- 2) Prohibits ISPs from engaging in certain activities that impact a consumer's ability to lawfully access content on the Internet, including, but not limited to the following:
 - a) Intentionally blocking lawful content, slowing or speeding traffic, or otherwise interfering with access to lawful content on the basis of source, destination, Internet content, application, or service, or use of a non-harmful device.
 - b) Engaging in third-party paid prioritization.
 - c) Selectively zero-rating some Internet content, applications, services, or devices or zero-rating in exchange for consideration or payment.
 - d) Engaging in practices that have the purpose of evading net neutrality requirements. This prohibition may not be construed as prohibiting ISP traffic exchange agreements that comply with net neutrality requirements.
 - e) Failing to publicly disclose accurate information about the network management practices, performance, and commercial terms of its broadband Internet access services to enable consumers to make informed choices about those services.
 - f) Requiring consideration from edge providers, monetary or otherwise, for access to an ISP's end users. (Civil Code §3101)
- 3) Prohibits mobile and fixed ISPs from offering services other than broadband Internet access service over last-mile connection if those other services can be used as an equivalent of broadband Internet and do at least one of the following:
 - a) Have the effect of evading net neutrality requirements or
 - b) Negatively impact the performance of broadband access Internet services. (Civil Code §3102)
- 4) Specifies that nothing limits ISPs from meeting the needs of emergency communications, law enforcement, public safety, or national security authorities. (Civil Code §3103)

This bill:

- 1) Prohibits mobile ISPs from impairing or degrading the lawful Internet traffic of first response agencies after receiving notification that the agency is responding to an emergency. After receiving this notification, mobile ISPs must lift data restrictions until the emergency ends or the telecommunications account is no longer used for emergency response, depending on which occurs earlier.
- 2) Makes this bill's prohibitions on impairing or degrading lawful Internet traffic subject to reasonable network management practices.
- 3) Authorizes first response agencies to request removal of data restrictions when responding to an emergency and requires these agencies to notify an ISP when the agency ceases to participate in the emergency response.
- 4) Requires first response agencies to provide the account number and lines for which they are requesting the removal of data restrictions.
- 5) Makes various definitions for the purposes of this bill, including defining an emergency for the purposes of the bill and specifying that certain terms have the same meaning as those terms are used for existing law regarding net neutrality.

Background

California's net neutrality requirements. Last year, the Legislature passed SB 822 (Weiner, Chapter 976, Statutes of 2018), which established net neutrality requirements within California. These requirements prohibit an ISP from engaging in activities that impair or degrade end user's ability to lawfully access Internet traffic. Specifically, the bill prohibits ISPs from blocking, throttling, engaging in paid prioritization, selectively zero-rating, and requiring consideration from edge providers to deliver content to end users. California's net neutrality provisions largely apply to fixed ISP connections; however, it prohibits mobile ISP from offering products that have the purpose of evading net neutrality requirements. This bill prohibits mobile ISPs from impairing or degrading a first response agency's lawful Internet access while the agency is responding to an emergency.

Throttling of firefighters during Mendocino Complex Fire response. While the Legislature was considering net neutrality requirements, the Santa Clara County Fire Department (SCCFD) filed a complaint in a federal court proceeding stating that Verizon throttled the SCCFD's data while the SCCFD was dispatched to provide mutual aid during the Mendocino Complex Fire. The SCCFD deployed an OES 5262 incident command truck that uses software to conduct real-time tracking

of resources responding to the fire. The truck's software relies heavily on the ability to send and receive large volumes of data when in use.

The SCCFD had a plan from Verizon that included unlimited data; however, the plan's terms permitted throttling when more than a certain volume of data is used during the monthly billing cycle. The throttling effectively limited the first responders' ability to use OES 5262 until it could resolve the data limitations. Once the SCCFD realized that its Internet data speed had slowed dramatically, it contacted Verizon to remove the data limit. However, Verizon did not immediately remove the data restrictions; instead, a customer service representative informed the SCCFD that it would need to upgrade the plan that cost more than double the SCCFD's existing monthly cost to prevent throttling. The SCCFD ultimately upgraded its plan and Verizon removed the throttling. After the SCCFD's complaint became public, Verizon apologized for the error and committed to taking steps to prevent throttling of public safety accounts in the future. In an August 2018, informational hearing held by the Assembly Select Committee on Natural Disaster Response, Recovery, and Rebuilding, representatives for Verizon discussed plans to establish a new program for public safety accounts that would not contain data limitations and would include priority data access at no additional cost.

This bill establishes a notification process for first response agencies to notify their respective mobile ISPs of the need to lift data restrictions when responding to disasters. Under this bill, a mobile ISP must lift data restrictions until the emergency ends or the telecommunications account is no longer used for emergency response, depending on which occurs earlier. A first response agency making a request must identify the account number and lines for which data restrictions should be removed. An agency that has made a request for removal of data restrictions must notify the mobile ISP once the agency ceases to respond to the emergency.

States of emergency. This bill does not require a state of emergency proclamation as a prerequisite for requesting removal of data restrictions; however, it defines an emergency for the purposes of this bill. This bill's definition of an emergency does not ensure that local agencies do not need to wait until an emergency is duly proclaimed to request the removal of data restrictions. Emergency proclamations frequently are not issued at the start of a local or state emergency. As a result, first response agencies may respond to an emergency for an extended duration of time before a proclamation of the emergency exists. First response agencies likely need data restrictions removed prior to the proclamation of an emergency. Local first response agencies may also cease to respond to an emergency prior to the declared

end of an emergency. This bill authorizes local agencies to request the removal of data restrictions when responding to an emergency and requires the agencies making these requests to notify their respective ISPs once they cease to respond to the emergency.

Related/Prior Legislation

SB 822 (Weiner, Chapter 976, Statutes of 2018) established net neutrality requirements in California by prohibiting ISPs from taking certain actions that interfere with consumers' ability to lawfully access Internet content, including impairing or degrading lawful Internet traffic. The bill prohibited intentionally blocking content, speeding up or slowing down traffic, engaging in paid-prioritization, requiring consideration from edge providers for access to an ISP's end users, and selectively zero-rating certain content.

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

SUPPORT: (Verified 9/5/19)

California Central Valley Flood Control Association
California Fire Chiefs Association
California Professional Firefighters
City of Thousand Oaks
County of Santa Clara
Electronic Frontier Foundation
Fire Districts Association of California
League of California Cities
Media Alliance

OPPOSITION: (Verified 9/5/19)

CTIA-The Wireless Association

ARGUMENTS IN SUPPORT: According to the author:

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 service provider, Verizon Wireless. 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.

ARGUMENTS IN OPPOSITION: CTIA, the trade association for the wireless communications industry opposes this bill. In opposition, CTIA states the following:

...our concern is the AB 1699 may have unintended consequences and could actually undermine, not aid, public safety access during emergencies. As such, CTIA opposes AB 1699 as drafted, but will continue to work with the author and public safety on our mutual goals.

ASSEMBLY FLOOR: 75-0, 5/9/19

AYES: Aguiar-Curry, Bauer-Kahan, Berman, Bloom, Boerner Horvath, Bonta, Brough, Burke, Calderon, Carrillo, Cervantes, Chau, Chiu, Choi, Chu, Cooley, Cooper, Cunningham, Daly, Diep, Eggman, Flora, Fong, Frazier, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Gloria, Gonzalez, Gray, Grayson, Holden, Irwin, Jones-Sawyer, Kalra, Kamlager-Dove, Kiley, Lackey, Levine, Limón, Low, Maienschein, Mathis, Mayes, Medina, Melendez, Mullin, Muratsuchi, Nazarian, Obernolte, O'Donnell, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Smith, Mark Stone, Ting, Voepel, Waldron, Weber, Wicks, Wood, Rendon

NO VOTE RECORDED: Arambula, Bigelow, Chen, Dahle, McCarty

Prepared by: Sarah Smith / E., U., & C. / (916) 651-4107
9/6/19 13:33:39

**** END ****

CONCURRENCE IN SENATE AMENDMENTS

AB 1699 (Levine)

As Amended September 5, 2019

Majority vote

SUMMARY:

Prohibits a mobile internet service provider from impairing or degrading the lawful internet traffic of first response agencies during an emergency.

The Senate Amendments:

Authorizes a first response agency to submit a request to a mobile internet service provider to not impair or degrade the lawful internet traffic of an account used by the agency in response to an emergency. Specifies that as part of the request, the first response agency shall identify the account number and lines for the mobile internet service provider.

Requires the first response agency that submits the specified request to notify the mobile internet service provider upon the account no longer being used by the agency in response to the emergency.

Makes additional technical and clarifying changes.

COMMENTS:

Throttling during Mendocino Fires: During the 2018 Mendocino Complex Fire, the Santa Clara Fire Department experienced a dramatic decrease in the data connection speed of their communications equipment to the point where it severally interfered with the Department's ability to function effectively. The Department contacted its internet service provider, Verizon, which told them that their service plan, while offering unlimited data, had a provision in which its data speed would decrease considerably once a certain threshold of data had been exceeded in a given billing cycle. The Department asked Verizon to end the throttling in light of the emergency situation, however, it only ended after the Department agreed to purchase another plan that included a higher data threshold. Following the incident, Verizon acknowledged that it had made a mistake and issued an apology.

According to the Author:

While combatting the Mendocino Complex Fire, Santa Clara County Fire officials experienced data throttling of mutual aid communications equipment by their telecommunications service provider, Verizon Wireless [...] 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, this bill will ensure the data throttling of public safety communications equipment is never repeated.

Arguments in Support:

According to the California Professional Firefighters, "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 [...] 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."

Arguments in Opposition:

According to CTIA, "Whether it is E911, location accuracy, Wireless Emergency Alerts, disaster response, or network resiliency, wireless companies work with public safety to ensure that wireless technologies are used effectively to keep Americans safe. We stand ready to continue this vitally important work with our public safety partners [...] Our concern is that AB 1699 may have unintended consequences and could actually undermine, not aid, public safety access during emergencies. As such, CTIA opposes AB 1699 as drafted, but will continue to work with the author and public safety on our mutual goals."

FISCAL COMMENTS:

Unknown. This bill has been keyed non-fiscal by the Legislative Counsel.

VOTES:

ASM COMMUNICATIONS AND CONVEYANCE: 12-0-1

YES: Santiago, Obernolte, Boerner Horvath, Bonta, Brough, Gipson, Holden, Kamlager-Dove, Low, Patterson, Quirk-Silva, Rodriguez

ABS, ABST OR NV: Cervantes

ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0

YES: Chau, Kiley, Bauer-Kahan, Berman, Calderon, Gabriel, Gallagher, Irwin, Obernolte, Smith, Wicks

ASSEMBLY FLOOR: 75-0-5

YES: Aguiar-Curry, Bauer-Kahan, Berman, Bloom, Boerner Horvath, Bonta, Brough, Burke, Calderon, Carrillo, Cervantes, Chau, Chiu, Choi, Chu, Cooley, Cooper, Cunningham, Daly, Diep, Eggman, Flora, Fong, Frazier, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Gloria, Gonzalez, Gray, Grayson, Holden, Irwin, Jones-Sawyer, Kalra, Kamlager-Dove, Kiley, Lackey, Levine, Limón, Low, Maienschein, Mathis, Mayes, Medina, Melendez, Mullin, Muratsuchi, Nazarian, O'Donnell, Obernolte, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Smith, Mark Stone, Ting, Voepel, Waldron, Weber, Wicks, Wood, Rendon

ABS, ABST OR NV: Arambula, Bigelow, Chen, Dahle, McCarty

SENATE FLOOR: 40-0-0

YES: Allen, Archuleta, Atkins, Bates, Beall, Borgeas, Bradford, Caballero, Chang, Dahle, Dodd, Durazo, Galgiani, Glazer, Lena Gonzalez, Grove, Hertzberg, Hill, Hueso, Hurtado, Jackson, Jones, Leyva, McGuire, Mitchell, Monning, Moorlach, Morrell, Nielsen, Pan, Portantino, Roth, Rubio, Skinner, Stern, Stone, Umberg, Wieckowski, Wiener, Wilk

UPDATED:

VERSION: September 5, 2019

CONSULTANT: Edmond Cheung / C. & C. / (916) 319-2637

FN: 0002238