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 --