California Broadband Internet Privacy Act

(Amended September 12, 2017)

The Real Facts Regarding AB 375

Here is the straight story around EFF's so-called AB 375 "*Myths vs Reality.*" EFF is a sponsor of AB 375 and has had more than 5 months following Congress' repeal of the controversial FCC Broadband privacy rule to develop a bill that avoids serious adverse consequences. In the last week of the session, EFF and the author have presented amendments that are designed to fix these problems, and EFF has now issued a myth-fact chart claiming to have fixed serious problems with the bill. However, these serious problems remain. The final column in the chart below sets forth the facts -- highlighting the serious and enduring flaws in AB 375 and in EFF's claimed myths and realities shown in the first two columns below.

AB 375 is not ready for prime time and should not be passed hastily in the final day of the session.

EFF'S *CLAIMED* "MYTH":	**EFF'S *CLAIMED* "REALITY":**	**IN FACT:**
A state-level ISP privacy bill would lead to a "patchwork" of state laws instead of a single, federal standard and rules that stop at the state line don't work in today's interconnected world.	The nation already had a single federal standard in the FCC Rules until the Trump Administration and the Republican Congress revoked them in April at the request of the ISPs. And without those Rules, a state patchwork of protections would be far better than no protection at all. However, two other states - Nevada and Minnesota – already have ISP privacy laws on the books, and the internet still works in Nevada, last we checked.	The claim that California needs to act now because currently there is "no protection at all" is simply false. The FCC's privacy rules *never* went into effect, *and all of the federal and state privacy laws that were in place before the congressional CRA action and on which the FCC and others relied to protect consumers during the FCC proceeding still apply.* So there is no privacy "gap" to fill in here; rather, consumers' privacy has been – and still is -- consistently and adequately protected "last we checked." Even FCC Commissioner Clyburn—a supporter of the FCC's rules—has acknowledged the obvious problem of different rules for different providers across different states, testifying recently before a House committee that "I don't think the American public would be very comforted to know that depending on who they call or who their provider is or where they go online that they might have different levels of expectations or protections." And those NV and MN state laws are more than 10 years old, not nearly as restrictive as this bill, and this bill would conflict with them.

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
		Passage of this bill would open floodgates of bills in other states. The FCC has a pending proposal that would restore the FTC as the federal privacy regulator of ISPs along with all other Internet entities. That is the best path forward here for consumers and for the Internet economy, and, notwithstanding the scare tactics and false claims of some, consumers remain protected by existing laws while the FCC and FTC implement this proposal.
The bill will impose onerous permission requirements on consumers, who will be annoyed by constant pop-up consent requests.	No. Consumers only need to consent to information use and sharing once, not every time they use the internet. And while ISPs are required to ask again if they materially change their use/sharing policy (like sharing new types of info with new types of outside companies), such changes are information consumers would want to know and are entirely under the ISP's control.	New requests for consent would be required for any use not specifically included in the initial request for consent. This would likely annoy consumers.
The bill will cause consumers to be vulnerable to cyberattacks	Absolutely not. Even though security measures would reasonably be a normal part of the provision of the service (Section22552 (a)(2)(C)) clearly gives ISPs the authority to further protect the rights and property of the provider and protect users and the provider from fraudulent, abusive or unlawful use of service – which includes cyber threats.	Easy to claim here, but that is not what the bill provides. The bill would bar ISPs from sharing any potentially identifiable information with law enforcement in many circumstances. For example, a threat to conduct a terror attack could not be shared (unless it was to protect *the ISP, its users, or other ISPs* from fraudulent, abusive, or unlawful use of the ISP's service). AND the bill instructs that all such exceptions are to be construed *narrowly*. In contrast, EFF has long opposed cybersecurity information sharing of IP addresses to protect consumers. Even the FCC saw the need to clearly

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
		exempt the use and disclosure of customer information for these important cyber-attack purposes, and it *expressly did so* in a separate portion of the FCC's Order – *yet the bill never even mentions these FCC statements.*
The bill will prevent retail companies like Starbucks or Southwest Airlines from providing wifi internet access to customers.	No. Such companies would not fall under the existing definition of a broadband provider, and to forestall any confusion, the bill explicitly excludes premises operators like coffee shops, bookstores, airlines, etc. (22551(c)(2))	The latest amendments would exempt *retail-based* Wi-Fi, but would impose all the bill's requirements on *free public* Wi-Fi, requiring cumbersome opt-in consent that would slow Californians' access to public Wi-Fi.
The bill is different from the FCC Privacy Rules.	There are some natural differences between AB 375 and the FCC rules because a broad federal regulation will always differ in details from a more narrow state statute. There were also many unnecessary provisions in the Rules that were duplicative of existing state law (like privacy policy disclosure, security requirements, and data breach notification). And, the bill purposely incorporates a new element that the Rules did not: a ban on pay-for-privacy schemes that unfairly make privacy a luxury, at the expense of those less wealthy. But, AB 375 and the Rules share the primary element of an opt-in consent requirement for use, disclosure or access of sensitive personal information for reasons other than service provision.	The bill is FAR broader than the FCC Privacy Rules. It contains an entirely new, *last-minute* definition of "sensitive information" in § 22551(m)(7)(B) that includes IP addresses and domain names as "sensitive information." The final FCC rules specifically chose to *exclude* from their opt-in requirement these *non-sensitive* data elements that routinely travel all over the Internet. AB 375 dramatically expands the opt-in requirement in its bill through this last minute change without any explanation or justification on why it chose to conflict with the FCC's Rules and Order on this key issue. Even more fundamentally, the Obama White House and the Obama Federal Trade Commission both concluded that web browsing and app usage information are *not* sensitive information unless they relate to health information or other sensitive data categories spelled out by the FTC. The so-called "pay-for-privacy" restriction, not found in the FCC Rules, equally

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
		prohibits ISPs from offering consumers *lower prices* or other incentives if they affirmatively consent to *clearly disclosed* uses of their data. That choice should be the consumers' not the CA legislature's. The FCC had studied this issue carefully and expressly found it should be permitted because these incentives *benefit* consumers. The bill, by contrast, eliminates this FCC finding.
*A **state** ISP privacy bill would be federally pre-empted anyway.*	That's highly debatable. The federal Communications Act does not expressly preempt states from engaging in and enforcing consumer privacy, and the FCC's own repealed rules actually expected states to do so. Furthermore, the fact that two states already have ISP privacy laws on the books (Nevada and Minnesota), and 20 more states have introduced bills on the topic this year, tells us that preemption is far from certain. However, ISP provider Verizon has requested that the FCC issue a rule to explicitly preempt state and local broadband ISP laws.	The Communications Act is not the issue. The CRA is. As the many sponsors of the joint CRA resolution stated, Congress disapproved of the FCC's 2016 rules because they exceeded congressional intent; conflicted with well-established federal policy supporting a technology-neutral privacy framework for ISPs and non-ISPs; were unnecessary, overly restrictive, and discriminatory; and would harm consumers. This legislative action under the CRA also expressly bars "substantially similar" rules absent future authorization by Congress, a ban which applies not only to federal laws but also necessarily extends to state laws under the Supremacy Clause—especially given the inherently interstate nature of the Internet. Congress's rejection of the FCC's privacy rules, in favor of a regulatory approach that "mirrors" and reaffirms the FTC's more balanced, technology-neutral privacy framework, is thus a clear statement of federal deregulatory policy and preempts conflicting state laws. By purporting to adopt substantially the same (and, in many aspects, more onerous)

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
		regulations as the disapproved FCC 2016 rules, AB 375 plainly conflicts with, and would frustrate, Congress' intent to establish a different *nationwide* privacy framework. Indeed, AB 375 does what the CRA resolution expressly *forbids*, by adopting substantially the same – and in some aspects *identical* – regulations as the repealed FCC rules.
		The Bill is therefore a ripe target for federal preemption under well-established Supremacy Clause principles. No state has passed an ISP privacy bill this year, and the prior FCC Rules' statement on preemption is legally irrelevant because Congress repealed it. But even if that statement *were* still applicable, it would also require preemption of the bill -- that prior statement only permitted states to adopt privacy laws that are *consistent* with federal law, and yet the bill is clearly *inconsistent* with the express intent and directives of Congress under the CRA.
Broadband providers shouldn't be treated differently from "edge providers" or any other company – they deserve a 'level playing field.'	Broadband internet service providers actually **are** different from edge providers and should be treated as such: • ISPs are regulated common carriers and have a higher set of responsibilities to their customers; edge providers are not. • High-speed ISPs face no competition in nearly half the state and are hard for consumers to switch; edge providers have lots of competition and consumers	The clearest evidence that the bill is fundamentally flawed is that, although it purports to regulate only ISPs, the opposition to the bill is broad and extensive – including ISPs; edge providers; retail, restaurant, insurance, and manufacturing associations; software and tech organizations; and a wide range of other state and local business groups. The sheer breadth of the companies in opposition speaks volumes about the potential negative impact the bill would have on consumers and the Internet economy, and the importance of taking the

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
	can switch easily (i.e. from Google to Yahoo to Bing, etc.) • ISPs are paid for their commodity service, while many edge providers are free – your information is the consideration for use of the service. • Consumers can use ad blocking and anti-tracking software to block edge provider targeted advertising, but have no technological means to block an ISP. • A majority of independent California ISPs support the bill.	time to get this right.
This bill will interfere with an ISP's ability to serve their customer normally or work with law enforcement in the event of an emergency.	No. AB 375 explicitly exempts from the consent requirement a wide variety of reasonable uses: anything necessary to the provision of the service, sign-up and billing, fraud detection and cyber security, first-party marketing, appropriate coordination with law enforcement (like 911 calls), the creation and use of aggregate data sets and non-personally identifiable information for marketing, and any other legal use.	The Bill is not nearly as clear on these issues as this advocacy piece blithely suggests; it will undoubtedly spawn costly and burdensome litigation over what is and is not allowed. Notice what EFF does *not* say: the bill *would* bar ISPs from sharing any potentially identifiable information with law enforcement in many circumstances. For example, a threat to conduct a terror attack could not be shared (unless it was to protect *the ISP, its users, or other ISPs* from fraudulent, abusive, or unlawful use of the ISP's service.) Also, ISPs could not use any identifiable information to innovate to provide new services. And again, the FCC's Order had contained many pages describing additional exemptions from the rules for research, product improvements, data analytics, etc. that the bill does not even mention.

EFF'S *CLAIMED* "MYTH":	EFF'S *CLAIMED* "REALITY":	IN FACT:
This bill was too rushed – we should wait until next year.	The bill is necessary this year because the ISPs are actively pushing the Trump FCC right now to issue a rule to preempt states from enacting their own ISP privacy protections – so California needs to make its voice heard before it's too late. Furthermore, AB 375 has already been in print for three months and passed through two Senate policy committees. It even provides a twelve-month delayed effectiveness date to give the industry more time to prepare for implementation.	This argument makes no sense. If California legislates now, preemption would become MORE likely. And if the FCC really is pursuing a rule that preempts state privacy laws, that is going to stop this law *regardless* of when the law is enacted. There is no rush on this issue: No existing harms to consumers have been cited by bill proponents, existing federal and state privacy laws continue to protect consumers, and ISPs have made additional public commitments to follow the FTC privacy framework that the AG's Office can *already* enforce *today* without the need for a new bill. This bill has been around for 4 months, was gutted at least twice, and was amended yet again at the last week of session with entirely new, critically important definitions that have not been the subject of a hearing or consideration by any substantive committee. It IS too rushed.