# Top Ten Reasons to Vote against A.B. 375

**Reason #1:** **A.B. 375 is a politically-driven measure that is totally unnecessary** and will harm – *not* benefit – California consumers and California's economy. It's not just ISPs that recognize this; the coalition opposed to A.B. 375 includes major edge providers such as Google and Facebook, the Internet Association; retail and restaurant associations, insurance companies, manufacturing associations, and software and tech organizations.

**Reason #2:** **A.B. 375 "solves" a non-existent problem**. Numerous California and federal laws *already* protect consumer privacy on the Internet, and all major ISPs have publicly pledged (1) that they will not sell or share individual browsing histories to third parties and (2) not to share customers' sensitive information (such as banking, children's, and health information) without affirmative, opt-in consent. These commitments can be enforced TODAY under current California and federal law. So claims that there is a privacy "gap" that California needs to fill are false.

**Reason #3:** **A.B. 375 risks impeding innovation in California.** A.B. 375 requires opt-in consent for use of a wide range of information (including non-sensitive information such as IP addresses and domain names) to innovate in creating new products or services. Information would need to be de-identified in all cases, adding expenses for ISPs large and small to innovate.

**Reason #4:** **A.B. 375 needlessly restricts voluntary sharing of cyber threat information**. ISPs could share cyber threat information with other ISPs, but could not work together and share information with law enforcement to combat collective problems – it's like telling federal, state, and local law enforcement to combat crime, but to do so without talking to or coordinating with each other. Even the FCC saw the need to clearly exempt the use and disclosure of customer information for these important cyber-defense purposes, and it *expressly did so* in its Order.

**Reason #5:** **A.B. 375 would prevent ISPs from sharing information about terror threats and other crimes with law enforcement.** The bill allows information sharing with other ISPs and information sharing with law enforcement where there is a threat to the ISP or its users, but not for other purposes, unless there is an express authorization to do that under some other provision of law. This would mean that ISPs who inadvertently learned of a rightwing extremist or other violent threat to the public at large could not share that information with law enforcement without customer approval. Even IP address of the bad actor could not be shared.

**Reason #6:** **A.B. 375 makes consumer privacy more complex and confusing to consumers**. Everyone agrees that consumers deserve a consistent and comprehensive regime to protect their online data. FCC Commissioner Clyburn (D) noted the obvious problem of different rules across different states, testifying before a U.S. 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." California consumers will be confused if this passes.

**Reason #7:** **A.B. 375 would disrupt routine Internet operations and hamper innovation.** In a hurried attempt to "fix" the bill, a new, last-minute definition of "sensitive" web browsing history now includes IP addresses and domain names as "sensitive information." This information routinely travels all over the Internet, and even the FCC's rules specifically chose to exclude from their opt-in consent requirement these non-sensitive data elements.

**Reason #8:** **A.B. 375 would actually harm consumers**. ISPs would be hamstrung in their ability to use information to innovate their products and provide new services. And many consumers would lose out on learning about discounts and other offers that would save them money. A.B. 375 bans ISPs from offering consumers *lower prices* or other incentives if they affirmatively consent to *clearly disclosed* uses of their data. That choice should be made by consumers, not the CA legislature. The FCC had studied this issue carefully and expressly found it should be permitted because these incentives could *benefit* consumers. The bill, by contrast, eliminates this FCC finding entirely.

**Reason #9:** **A.B. 375 is a ripe target for federal preemption under well-established Supremacy Clause principles.** Congress's rejection of the FCC's privacy rules was a clear statement in favor of the FTC's comprehensive, technology-neutral privacy framework. And Congress also forbade adoption of "substantially similar" laws. AB 375 is actually the sort of requirement Congress intended to stop.

**Reason #10:** **A.B. 375 is not needed at all, much less right now, as the sponsors have acknowledged.** As amended, this bill doesn't even go into effect until January 2019. It is a rush job and deeply flawed – *Californians deserve better*. The FCC has a pending proposal that would restore the FTC as the federal privacy regulator of ISPs and non-ISPs. 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.