



Internet Association



TechNet



State Privacy and Security Coalition, Inc.

April 7, 2016

The Honorable Ed Chau  
California State Assembly  
Capitol Building, Room 2179  
Sacramento, CA 95814

**RE: AB 1681 (Cooper) - Mandate to weaken smartphone security  
As amended March 28, 2016  
OPPOSE**

Dear Assemblymember Chau:

We are writing to express our unified **opposition to AB 1681 (Cooper)**, which would weaken smartphone security by punishing California companies if they do not fundamentally and negatively alter the robust protections that are currently standard on millions of smartphones. While we support the author’s goal of combating human trafficking and other heinous crimes, AB 1681 is the wrong approach. We respectfully urge your NO vote on the measure. Here is a summary of our concerns:

- **AB 1681 undermines data security.** There is no way to build a “back door” into a smartphone that can only be used by one person. Once a vulnerability exists, any party that discovers it – including criminals – can exploit it to bypass device security and access sensitive data. Foreign governments, including repressive regimes, can assert the same right to use that vulnerability as U.S. law enforcement agents. AB

1681 undermines efforts to make sure this data is as safe as possible by continuing to improve encryption and data security.

- **AB 1681 cripples innovation.** Under the language of AB 1681, smartphone manufacturers and operating service providers are liable if they cannot decrypt a smartphone upon demand — even if the device has been encrypted through software installed by the user. This means companies would have to lock down devices so that users cannot install third party software that might prevent decryption. This would cripple innovation in smartphone operating systems and applications.
- **AB 1681 ignores the reality of mobile phone theft and user safety/security.** According to *Consumer Reports*<sup>i</sup>, there were nearly 3.1 million victims of smartphone theft in 2013, nearly doubling the number of victims in 2012. That number fell to 2.1 million in 2014 after many smartphone manufacturers and software companies—at the request of law enforcement authorities—deployed kill switch technology. Strong encryption is intrinsic to these protections, as without it, they are more easily compromised.
- **AB 1681 is a mandate to weaken consumer protection.** As more of our lives move to mobile phones — via email, photo sharing, social networks, maps and geolocation — the need to protect these devices grows. Identity theft continues to be a significant problem<sup>ii</sup>. To help combat these issues, the Federal Trade Commission (FTC) has long called for encryption and continues to do so — by bringing law enforcement actions against companies who failed to use it effectively. While device owners rely on mobile phone encryption to deliver services, business both small and large do so as well. The payment and user authentication credentials that enable services that banks, online stores and app creators rely on will only be available if devices are secure.
- **AB 1681 contradicts recent policy changes.** In 2014, California enacted SB 962 (Leno), a measure requiring smartphones to include technological solutions capable of rendering the device inoperable to unauthorized users (e.g. kill switches). Supported by law enforcement, the measure was in response to a stated “epidemic” of smartphone theft. Underscoring the Legislature’s desire for strong kill-switches, the bill specifically required the technology to be “capable of withstanding a hard reset or operating system downgrade”—two common methods, as the proponents of SB 962 held, that criminals use to work around security features. In stark contrast to the Legislature’s approach with SB 962 (Leno), AB 1681 (Cooper) would essentially require manufacturers and operating system providers to invite criminals to rediscover value in these devices through mandated security vulnerabilities.
- **AB 1681 fails to achieve its public safety objectives.** While perhaps well-intentioned, AB 1681 will do nothing to further the author’s stated goal. Even if all smartphones in California had their security fundamentally weakened as this bill envisions, criminals could still use a phone obtained outside California or bypass any prohibitions on third-party software and layer on some of the strongest open-source encryption technology available to anyone on the Internet<sup>iii</sup>. Weakening the security of the mobile phone ecosystem would not stop bad actors seeking to hide their

actions. However, such a mandate would pose significant harms to the most vulnerable, law-abiding Californians.

- **AB 1681 sets a dangerous precedent.** As a trend-setting state that often leads the nation in protecting consumers, we are gravely concerned about the precedent this bill could set. The enactment of AB 1681 would represent a first-of-its-kind mandate essentially making it easier and more defensible for governments to weaken important consumer protections across other types of devices, technologies, and data. This would increase cyber risk to consumers and make it easier for hackers and criminals to exploit online.

We appreciate your consideration of our perspective and hope you will **vote NO on AB 1681 (Cooper)**. We would be happy to answer any questions you have about our views.

Sincerely,

Application Developers Alliance  
ACLU of California  
California Bankers Association  
CalChamber  
Center for Democracy & Technology  
CompTIA  
CTIA  
Electronic Frontier Foundation  
Google  
Internet Association  
NetChoice  
Silicon Valley Leadership Group  
State Privacy & Security Coalition  
TechNet

cc: The Honorable Jim Cooper, California State Assembly  
Members, Assembly Privacy & Consumer Protection Committee  
Hank Dempsey, Chief Consultant, Assembly Privacy & Consumer Protection Committee  
Jared Yoshiki, Consultant, Assembly Republican Caucus

---

<sup>i</sup> <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>

<sup>ii</sup> [https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints?utm_source=govdelivery)

<sup>iii</sup> <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>