April 4, 2016

VIA FAX AND US MAIL

Ed Chau, Chair
California State Assembly
Privacy and Consumer Protection Committee
Room 156A, Legislative Office Building
1020 N Street
Sacramento, CA 95814

Members: Assemblymembers Scott Wilk, Catharine Baker, Ian Calderon, Ling Ling Chan, Jim Cooper, Matthew Dababneh, Mike Gatto, Richard Gordon, Evan Low, Kristin Olsen

Re: Letter of Opposition to AB 1681

Dear Assemblymember Chau and Honorable Members of the Privacy and Consumer Protection Committee:

As members of the Oakland Privacy Working Group ("OPWG"), we write to express our strong opposition to AB 1681. If adopted, AB 1681 will prioritize surveillance capabilities at the expense of benefits to security and free speech. Furthermore, the bill itself does nothing to prevent human trafficking or help its victims.

OPWG is a citizen's coalition that works regionally to defend the right to privacy and enhance public transparency and oversight regarding the use of surveillance techniques and equipment. We were instrumental in the creation of the first standing municipal citizens' privacy advisory commission in the City of Oakland, and we have engaged in successful privacy enhancing legislative efforts with the Alameda County and Santa Clara Boards of Supervisors, as well as the California State Legislature.

AB 1681 proposes to fight human trafficking by penalizing full-disk encryption (FDE) and assessing a $2,500 civil penalty upon any manufacturer of a smartphone that uses FDE and cannot make available the full contents of a phone in response to a court order. This is a wrongheaded approach for many reasons.

I. A Backdoor For One Is An Opening For All.

When the NSA, ACLU, and Silicon Valley are telling you the same thing, it would be wise to listen.[1] As prominent technologists have agreed with a remarkable level of unanimity, robust encryption provides valuable protection for smartphone users. Phones are high value devices that provide profound insights into peoples' lives, social networks, medical histories and private conversations. Phone data is targeted by a variety of actors including:

- Criminal cons and attempted fraudulent scams including identity theft
- Stalkers
- Business competitors including vulnerable whistleblowing individuals
- Abusers in domestic violence
- Foreign intelligence organizations

Robust encryption of smartphone devices was developed specifically to protect smartphone users from all of these threats in response to consumer demand and the needs of the marketplace. This bill proposes to financially penalize manufacturers on the occasions when law enforcement is unable to compel a user to unlock or de-encrypt their phone by encouraging an approach called key escrow. Key escrow introduces vulnerabilities into the cryptosystem that can be exploited by bad actors in difficult to imagine ways. The belief of the experts in the field of computer security is that such actions fundamentally compromise the security offered by encryption. [2]

Former California state Senator, and current House of Rep. Ted Lieu is one of a handful of legislators with a computer science degree and a keen technical understanding of the issue. "It's very clear to me that the people who are asking for a backdoor encryption key do not understand the technology," he added. "You cannot have a backdoor key for the FBI. Either hackers will find that key or the FBI will let it get stolen. As you saw, the [DOJ] got hacked. The [Office of Personnel Management] got hacked multiple times. If our federal government cannot keep 20 million extremely sensitive security records, I don't see how our government can keep encryption keys safe."[3]

As an example of the risks inherent in well-intended anti-encryption efforts, a key escrow mechanism inside Juniper routers was purposed by an unknown entity for widespread interception of confidential government data.[4] The mind boggles at the potential for harm if FDE is compromised for all iPhone and Android users. In other words, the proposed remedy for the frustrating times when law enforcement has difficulty accessing some smartphone contents in a criminal investigation can have broad unanticipated side effects across the entire spectrum of smartphone users and all electronic data.

II. The Need For Encryption

The nexus between freedom of expression and encryption is more important and relevant than ever. In their February 10, 2015 comments to the UN Special Rapporteur on the Promotion and Protection of

---

[1] National Security Agency Director Adm. Mike Rogers - "encryption is foundational to the future,"; Former NSA director, Michael Hayden - "I disagree with Jim Comey. I actually think end-to-end encryption is good for America." https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/.

2 https://dspace.mit.edu/handle/1721.1/97690

[3] http://linkis.com/arstechnica.com/tech/AZk4r

4 http://www.wsj.com/articles/the-data-breach-you-havent-heard-about-1453853742

the Right to Freedom of Opinion and Expression, the ACLU stated:

> "First, encryption and anonymity are the modern safeguards for free expression. Without them, online communications are effectively unprotected as they traverse the Internet, vulnerable to interception and review in bulk. Encryption makes mass surveillance significantly more costly, and anonymity allows dissidents, whistleblowers, and human rights defenders to freely express themselves, organize, and expose governmental abuse without fear of retribution. Second, and equally importantly, strong encryption is essential to cybersecurity. Over the last few years, hackers and repressive regimes have unleashed increasingly devastating cyberattacks on companies around the world, including American companies that hold the sensitive financial, medical, and other data of millions of individuals. Strong encryption is our best defense against the growing threat of such cyberattacks."[5]

In 2014, hundreds of millions of US business and government customers had their data stolen.[6] Ethiopia, one of the most egregious state actors, jailed six bloggers for attending a digital security training where they learned about basic encryption.[7] Encryption enhances both political freedom and security from criminal wrongdoing.

III. The Proposed Bill Will Not Serve Its Intended Purpose.

In announcing his proposal, Assemblymember Jim Cooper stated that "[h]uman traffickers are using encrypted cell phones to run and conceal their criminal activities. Full-disk encrypted operating systems provide criminals an invaluable tool to prey on women, children, and threaten our freedoms while making the legal process of judicial court orders useless."[8] It is noteworthy that he offered no authority for his conclusions. As we learned after the initial knee-jerk reaction to the Paris terrorist attacks and subsequent call to ban encryption in France, those attackers didn't use encryption.

The text of AB 1681 cites long discredited human trafficking statistics, including that there are over 100,000 children being trafficked in the US. This figure arose from Ernie Allen's 2010 congressional testimony. Mr. Allen was the President for the National Center for Missing and Exploited Children ("NCMEC") at that time. Mr. Allen now admits that there is "no scientific empirical data" about the number of children in the sex trade.[9] In 2014, NCMEC said it received reports of about 1,800 children linked to sex trafficking, and a spokeswoman said the organization no longer uses the figures created by its former president.[10] Assemblymember Cooper's announcement was timed to coincide with the 2016 Super Bowl, and belies another discredited myth of the human trafficking trade – that sporting events cause a spike in human trafficking.[11]

---

[5] https://www.aclu.org/sites/default/files/assets/aclu_submission_to_special_rapporteur_-_encryption_and_anonymity.pdf
[6] https://spideroak.com/articles/10-notable-privacy--security-breaches-of-2014--tips-to-secure-your-data
[7] http://www.huffingtonpost.com/pen-american-center/in-ethiopia-protecting-yourself-online-is-a-crime_b_5611017.html
[8] http://asmdc.org/members/a09/news-room/video-gallery/cooper-introduces-human-trafficking-investigation-legislation
[9] https://www.washingtonpost.com/news/fact-checker/wp/2015/09/02/the-fishy-claim-that-100000-children-in-the-united-states-are-in-the-sex-trade/
[10] Ibid.
[11] http://www.huffingtonpost.com/entry/super-bowl-sex-trafficking-harmful_us_56b4e08be4b08069c7a7068b

We fail to see how this bill will help prohibit the real human trafficking that does exist. As a former law enforcement official, Assemblymember Cooper perhaps unwittingly revealed at his press conference what works when it comes to solving human trafficking crimes – human intelligence, and lawful use of unencrypted metadata, such as the parties and phone numbers called.[12] The NSA agrees with him.[13] It must be pointed out that the FBI did not need Apple to crack the "San Bernardino" phone, as it originally claimed.

It has been stated that we are living in a 'golden age of surveillance' due to the many online and smartphone activities we perform each day. Phone records can trace our steps, and our online footprints are just as revealing. Only the most sophisticated of criminal masterminds can hide their electronic footprints in this modern era, and there is no evidence that human traffickers possess these capabilities. To diminish the security of most to defeat a problem that may not exist is nonsensical. With AB 1681 stopping at the California border, fully encrypted phones will remain available for sale in neighboring states like Oregon or Nevada to California buyers. Numerous third party applications exist to add FDE functionality. According to the Electronic Frontier Foundation, over two thirds of these applications are created at least partially outside the United States[14] and cannot be regulated by state law. Furthermore, plenty of encryption technology is now open-source. Attempting to close the barn doors after the horses have left is pointless.

We also question the fairness of the proposed legislation. As premium manufacturer Apple has already demonstrated, it is likely that many of the most prominent manufacturers of smartphone devices may choose to simply pay the civil penalties mandated by AB 1681, rather than make changes to their encryption protocols. Apple has demonstrated the commitment of significant resources to resisting such demands and they have received support from other smartphone manufacturers including Google, Microsoft and AT&T [15].

If the California smartphone manufacturers most likely to be unable or unwilling to absorb the civil penalties are the smaller ones, then the proposed bill will have a disproportionate security impact on poor people who buy cheaper off-brand phones, while those who buy expensive premium smartphones will have their privacy protected - a two-tier system penalizing low income consumers. We object to decreased privacy protections for users with less income to devote to expensive and more secure electronics. State legislation leading to such a two-tier system will necessarily target low-income consumers, risk their electronic safety, potentially significantly raise their vulnerability to scams, identity theft, stalking and online harassment, and provide material threats to survival in the cases of domestic abuse and hate crimes, simply because they can only afford a cheaper, less secure smartphone.

Finally, there is no mechanism in the bill that even vaguely purports to help human trafficking victims. The 'tax' on secured phones will not be routed to any victim's compensation fund, rehabilitation services, or campaign to raise awareness. It is a thinly disguised money grab that will only make our

---

[12] http://asmdc.org/members/a09/news-room/video-gallery/cooper-introduces-human-trafficking-investigation-legislation , video at 0:48.

[13] Former NSA Director Michael Hayden has also spoken about how U.S. intelligence agencies have figured out how to get the information they need without weakening encryption — such as using metadata, which shows who is contacting whom. https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/

14 https://www.schneier.com/cryptography/archives/2016/02/a_worldwide_survey_o.html

15 https://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

communications less secure, while not achieving its stated goal.

For all of these reasons, OPWG strongly opposes AB 1681 and respectfully requests the members of the committee to vote against it.

Oakland Privacy Working Group
https://oaklandprivacy.wordpress.com/