The Digital Security Commission Act of 2016

The Center for Democracy & Technology's Response and Recommendations

May 6, 2016

The Center for Democracy & Technology (CDT) has reviewed and prepared recommendations for the Digital Security Commission Act of 2016 (S. 2604/H.R. 4651), sponsored by Senator Mark Warner and Representative Michael McCaul. The Act would establish in the legislative branch the National Commission on Security and Technology Challenges, which would be made up of experts from national security and law enforcement, the technology sector, and the cryptography and privacy and civil liberties communities. Within twelve months after its initial meeting, the Commission would be required to submit to Congress a final report on its findings and recommendations with regards to the benefits and challenges posed by digital security mechanisms.

Although CDT agrees with the general notion that bringing diverse stakeholders to the table is an important and effective means of solving a problem, and appreciates the effort that has been made to have a wide range of views present in the discussion, CDT cannot support this bill. Our principle concern is that the Commission's recommendations may lead to legislative and policy changes that leave everyone less secure. Moreover, the issue that the Commission is charged with tackling (how to realize the benefits of digital security technologies such as encryption while enabling law enforcement, intelligence, and other governmental agencies to bypass them) is an issue that has already been debated extensively. From the original "Risks to Key Escrow" paper that CDT coordinated in 1997 to the "CALEA II" paper that CDT organized in 2013, technology experts and policy advocates have consistently maintained that a backdoor to encryption is as dangerous as it is impracticable. Experts at Harvard, MIT, and within the President's Review Group agree. Therefore, it is hard to envision what a new Commission focused on old, well-settled issues can hope to accomplish. All of this is not to say that the sponsors of the bill envisioned key escrow to be the solution; throughout this process, Senator Warner and Representative McCaul have attempted to provide a balanced approach to their proposed Commission. However, the pressure to find a "solution" to the so-called encryption "problem" is at an all-time high, and CDT believes the dangers of the Commission endorsing a solution that puts all internet users at risk are far too great.

In the event that Congress fails to reject this legislation in its entirety, CDT's recommendations below may be used to mitigate some of its potential consequences. However, these recommendations should not be interpreted to mean that, if these changes are adopted, CDT will lend its support to the final bill. When it comes to encryption and the digital security of all internet users, CDT fundamentally believes that exceptional access of any type will leave us less secure. Instead, a commission aimed at finding ways for law enforcement to adapt to the technical reality of increasingly universal encryption might provide a more useful path forward.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. Section 3(b)(2)(B): Requiring the Commission to Conduct a Qualitative and Quantitative Assessment of . . .

> Section 3(b)(2)(B)(iv): *" . . . the effects of the use of cryptography and other digital security and communications technology on Federal, State, and local criminal investigations and counterterrorism enterprises."*

Any examination of the effects of the use of digital security technologies on law enforcement and counterterrorism should take into account investigative capabilities *in spite of* such security technologies. First, in order to understand the true impact of technologies such as encryption, there must be an understanding of how the U.S. government has been able to undermine the use of cryptography. In 2013, for example, the *New York Times* reported that the N.S.A. had been lobbying industry to weaken encryption standards, changing the design of cryptographic software, and encouraging the use of international encryption standards that it knew it could circumvent, then paying a major cryptographic software provider to use a compromised technology by default. The Commission should be charged with reporting publicly on such US government efforts to undermine encryption.

Moreover, the Commission should account for the new, alternative sources of information for investigations that result from the increasingly interconnected nature of devices, apps, and the Internet of Things (IoT) – rather than focusing solely on the techniques that may be *lost* because of encryption. A recent study by Harvard's Berkman Center for Internet and Society, for example, found that still images, video, and audio captured by networked sensors and the Internet of Things may provide alternative channels for surveillance, replacing prior channels that are now indecipherable due to encryption.

In short, CDT is worried that any study the Commission produces will focus only on the consequences of encryption rather than the ways in which law enforcement, intelligence, and other government agencies have been adapting to, and are aided by, the availability of information in digital world. Statutory language, legislative history, or both should reflect the intended scope of this study, which should encompass the effects of encryption by considering tools that undermine encryption or provide alternative avenues for surveillance.

II. Section 3(b)(2)(C): Requiring the Commission to make recommendations for policy and practice, including, if it determines appropriate, recommendations for legislative changes regarding . . .

> *Section 3(b)(2)(C)(i): " . . . methods to be used to allow the United States Government and civil society to take advantage of the benefits of digital security and communications technology while at the same time ensuring that the danger posed by the abuse of digital security and communications technology by terrorists and criminals is sufficiently mitigated."*

This language should be eliminated, because the "methods" that the Commission is being called on to recommend do not exist. It is simply not possible to ensure that civil society enjoys the full benefit of digital security mechanisms such as encryption while mitigating the effect those mechanisms have on the government's ability to read content of terrorists and criminals. The problem with backdoors and other exceptional access mechanisms is that, in the digital world, it is impossible to perfectly control who goes through them – if a backdoor is created for the government, it can be used by hackers, identity thieves, terrorists, and foreign governments, as well.

CDT recommends removing this language, unless lawmakers are willing to clarify that the means of "mitigating" the abuse of digital security and technology must: (i) exclude measures that diminish the benefits to civil society of digital security and technology, and (ii) include adaptation by taking advantage of new surveillance opportunities (as suggested in CDT's comments to Sec. 3(b)(2)(B)(iv), above).

> *Section 3(b)(2)(C)(ii): " . . . the tools, training, and resources that could be used by law enforcement and national security agencies to adapt to the new realities of the digital landscape."*

This provision correctly recognizes that law enforcement and national security agencies must adapt to a world in which digital security technologies such as encryption are becoming more universal. Banning some types of encryption or weakening encryption in the United States will not prevent individuals from obtaining encryption products from foreign sources. Such foreign sources are abundant – in a recent study of worldwide encryption services, 865 hardware or software products were identified, and two-thirds of those products came from outside the United States. Moreover, strong end-to-end cryptography is regularly taught to computer science students in undergraduate coursework, making the capabilities to engineer secure communications tools widely available. Therefore, any attempts to "mitigate" the effects of encryption by weakening it on the domestic front will be futile, and law enforcement must adapt by turning to security gaps left in systems that are difficult or impossible to upgrade.

However, CDT is concerned that law enforcement may choose to "adapt" by resorting to means that will result in decreased user trust in electronic devices and in communications technologies. This will lead to less security for devices, apps, and electronic communications. If, for example, law enforcement officials begin pushing to users exceptional access software that masquerades as a legitimate "software update," users may opt-out of any future updates, even those that contain important security upgrades. Therefore, CDT recommends amending this language to read as follows: " . . . the tools, training, and resources that could be used by law enforcement and national security agencies to adapt to the new realities of the digital landscape *without diminishing user trust in their devices, apps, and updates*."

> *Section 3(b)(2)(C)(iii): " . . . approaches to cooperation between the Government and the private sector to make it difficult for terrorists to use digital security and communications technology to mobilize, facilitate, and operationalize attacks."*

As discussed above, it is impossible to make digital security, or the internet, accessible to law-abiding users but not to terrorists and criminals. In addition, this provision contains very serious free-speech implications because it may lead to online service providers acting as law enforcement watchdogs, which would create a chilling effect on the free flow of their users' thoughts, ideas, and opinions. Previous legislative proposals aimed at channeling the private sector's capabilities towards preventing terrorists' use of their services would have put the private sector in the inappropriate position of deciding what sort of online activity counts as protected political advocacy and what should be categorized as terrorist activity. It is unclear, from this bill's language, how the Commission could solve this problem.

Given the technological infeasibility and the First Amendment difficulties of conscripting the private sector to do the government's bidding in this area, CDT recommends that this provision be removed and replaced. The alternate language should shift the focus away from making it "difficult" for certain people to use digital security and communications technologies and towards: (i) using technology to create counter-messaging campaigns that combat online propaganda by Islamic State and other terrorist groups; and (ii) identifying US government policies that support and enable speakers with alternative viewpoints, including journalists and activists, to express their views in the US and abroad.

> *Section 3(b)(2)(C)(iv): " . . . any revisions to the law applicable to wiretaps and warrants for digital data content necessary to better correspond with present and future innovations in communications and data security, while preserving privacy and market competitiveness."*

Privacy should be of utmost concern when updating wiretap and warrant laws – not an afterthought. Laws on the books and the court cases interpreting them have consistently lagged behind technological progress, leaving individuals not as protected from invasive searches and seizures of their digital content as they might expect. For example, according to the Supreme Court case *Smith v. Maryland*, an individual does not have a reasonable expectation of privacy in information they give to a third party. However, pending legislation such as the Email Privacy Act, which recently passed by unanimous vote in the House of Representatives, amends the 30-year-old Electronic Communications Privacy Act (ECPA) in a way that finally rejects the notion that law enforcement should not have to obtain a warrant when users "give" their emails, photographs, and other digital content to cloud service providers such as Google and Facebook. The Email Privacy Act's rejection of ECPA's 30-year-old rules for obtaining digital content is the perfect example of why the real focus should be on updating wiretap and warrant laws to better reflect the expectation of privacy that users have for their data in the 21st century.

CDT recommends reversing the order of priorities in this provision so that it reads, " . . . any revisions to the law applicable to wiretaps and warrants for digital content necessary to better *preserve privacy*

and market competitiveness, while *accounting for present and future innovations in communications and data security*."

> *Section 3(b)(2)(C)(v): " . . . proposed changes to the procedures for obtaining and executing warrants to make such procedures more efficient and cost-effective for the Government, technology companies, and telecommunications and broadband service providers."*

The warrant requirement is a key privacy protection. Although CDT is open to improved technological solutions that allow law enforcement to better track and serve warrants, we are concerned that the only metric the Commission is considering here is efficiency. It is important that overboard warrant requests and procedures for handling irrelevant or stale information secured through a warrant also be part of the Commission's remit. For example, in the case *United States v. Ganias*, the government seized computer hard drives and retained data on those hard drives beyond the scope of its original warrant for a period long after that warrant was effectuated. It later obtained a new warrant and used that nonresponsive data as evidence to prosecute a different crime. Retaining that data for future use might have been convenient for the government, but it also arguably violated the Fourth Amendment's particularity requirement and Mr. Ganias's right to be free from unreasonable intrusion into the privacy of his papers.

CDT has several recommendations for this provision. First, in order to narrow its extremely broad scope, it should be clear that the provision only applies to electronic data, and language relating to "obtaining" warrants should be eliminated. In addition, the provision should be amended to focus more on privacy, and particular consideration should be given to minimizing the impact of digital searches on privacy. Seizing an entire communications stream or all information in a person's online accounts has an increasingly dramatic impact on that person's privacy, and on the privacy of those with whom he or she communicates. Amended language could look like this: " . . . proposed changes to the procedures for ~~obtaining and~~ executing warrants *for electronic data to make those procedures more protective of privacy of targets and non-targets alike*."

> *Section 3(b)(2)(C)(vi): " . . . any steps the United States could take to lead the development of international standards for requesting and obtaining digital evidence for criminal investigations and prosecutions from a foreign, sovereign State, including reforming the mutual legal assistance treaty process, while protecting civil liberties and due process."*

CDT recommends removing this provision entirely because the topic of MLAT reform and cross-border data requests is far too complex for the Commission to adequately tackle within its twelve-month deadline, given the scope of its remit. CDT has already been working on this topic for years with several government, industry, and civil society stakeholders, and the various blog posts that CDT has published just within the past few months demonstrate the many difficult, interrelated issues that will have to be addressed in this area. It would be best to remove this provision from the Commission's already crowded plate of mandates.

III. Section 4: Composition of Commission

The Commission's composition is weighted in favor of national security, law enforcement, and corporate interests. Under the proposed bill, the Commission would be comprised of 16 members, 6 of which would represent corporate and economic interests, 6 of which would represent national security and law enforcement, and only 4 of which would represent cryptographers and privacy advocates. As a result of the bill's supermajority requirement, 5 votes are needed to block questionable recommendations and subpoenas, leaving cryptographers and privacy advocates – who are likely to be the strongest privacy proponents on the Commission – unable to block privacy invasive recommendations.

CDT recommends adding two more people to the Commission. These people should come from the civil rights community and reflect the interests of those who are disproportionately likely to be targeted for invasive government surveillance, such as Muslims and African Americans. The supermajority vote should correspondingly be changed to 14/18, which would require that Commission recommendations have the support of at least two members chosen because of their expertise in cryptography, privacy, or civil rights.

IV. Section 6(b): Powers of the Commission – Subpoenas

The subpoena power granted to the Commission by this bill is too broad, and CDT worries that this power will be susceptible to abuse. Under the bill's current language, the Commission would have the power to subpoena any information it considers "materially relevant" to its duties. As the ACLU has pointed out, "materially relevant" information could include the technical specifications of encrypted products or ways in which journalists use encryption to communicate.

As lawmakers move forward with amending the bill, they should consider ways to reign in this potentially vast power, without undermining the independence of the Commission and its ability to obtain the information it needs from law enforcement and intelligence community officials, including information that is classified. One approach would be to limit the subpoena authority to information held by government officials.

V. Conclusion

As we stated at the outset, CDT does not believe that the Commission envisioned in this legislation is necessary, and it has concerns that the Commission's recommendations will include ideas that undermine, rather than enhance, digital security and communications privacy. Adoption of the suggestions we have made would improve the bill, but not so much as to result in CDT's support for the legislation because our concerns about it are so fundamental.

For more information, please contact Joe Hall at jhall@cdt.org, (202) 407-8825, or Jadzia Butler at jbutler@cdt.org, (202) 407-8839.


CENTER FOR
DEMOCRACY
& TECHNOLOGY