

THE NATIONAL SECURITY PROGRAM

# **Weakened Encryption: The Threat to America's National Security**

By Mieke Eoyang, Vice President for The National Security Program and Michael Garcia, Senior Policy Advisor for The National Security Program

## **Takeaways**

For years, law enforcement officials have warned that, because of encryption, criminals can hide their communications and acts, causing law enforcement to struggle to decrypt data during their investigation—a challenge commonly referred to as “going dark.” They called on technology companies to build a process, like a “master key,” to enable law enforcement to unlock encrypted communications. While this may seem like a tempting idea, it would have grave implications for our national security. As more and more of our communications move online, users seek out encrypted services to protect their privacy. Unlike telephonic communications, and despite repeated requests by law enforcement to do so, Congress has not required internet communications platforms to give law enforcement access to intercept user communications or access stored communications. In this paper, we assess the national security risks to a requirement to provide that master key (referred to throughout as “exceptional” or “backdoor” access) to encrypted communications and propose alternative approaches to address online harms.

In short, requiring exceptional access to encrypted technologies would undermine national security by:

1. Weakening protections for the information that the national security community relies upon, especially as it flows over foreign networks.
2. Creating a vulnerability in encrypted communications that could be accessed by foreign adversaries.
3. Encouraging other countries to require tech and internet companies to provide equivalent access to communications within their boundaries.

This does not mean that the internet should be a lawless zone. Law enforcement and the private sector can and should cooperate in addressing crimes on the internet and can do so without undermining a protection as fundamental as encryption.

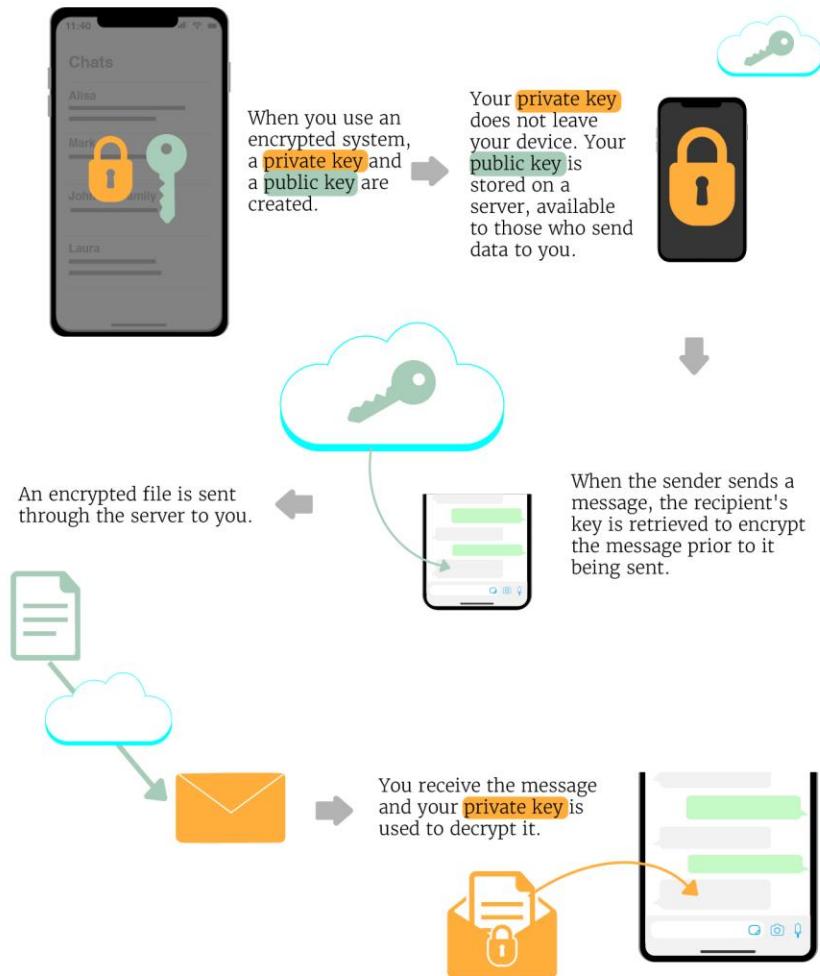
## How Encryption Works

Two forms of encryption generally exist that protect two types of data: “data in motion” and “data at rest.”<sup>1</sup> Encryption protecting data in motion (e.g., sending text messages) is a method of encoding information to ensure that only the sender and the recipient of a piece of information can view and read the information. If another party, such as the service provider or app developer, tries to read the information while it is in transit it will appear as a random collection of letters and numbers. This is often referred to as end-to-end encryption or E2EE. Similarly, encryption of data at rest protects communications that are stored on a device by securing a device's operating system, apps, or files by making it unintelligible to anyone who does not have the key to unscramble it.

Americans have reaped the benefits of encryption for centuries, and it currently provides them privacy from prying eyes, while protecting information pertinent to US national security. Leaders of the American Revolution did not just use invisible ink to hide their messages; they relied on ciphers—or codes—to protect their communications.<sup>2</sup> 21<sup>st</sup>-century encryption uses mathematical equations to “scramble data” so that only people with the right mathematical value (i.e., key) can unscramble and understand the information.<sup>3</sup>

Unless a third party can ascertain the key, using something like a “brute force” attack to guess every possible combination of mathematical values, only holders of the key (typically the sender and recipient) can decrypt and understand the information.<sup>4</sup> This means that no one else can read the information, not even the service provider or device manufacturer. Hundreds of millions of Americans enjoy the benefits of E2EE when using private messaging or video services like WhatsApp, Signal, and FaceTime.<sup>5</sup>

## How Encryption Works for Data in Motion



**Source:** <https://marktugbo.com/2019/04/06/infographics-end-to-end-encryption/>

 **THIRD WAY**

## How Encryption Works for Data at Rest



When storing data on an encrypted device, the data is unreadable to anyone while it is locked and can only be unlocked with the user's **private key**.



The user of the device can unlock or decrypt it by using their personal key. Only the user has access to this **private key**.



When the user unlocks the device, the data stored on it becomes readable.

★ **THIRD WAY**

## What Encryption Protects

Encryption has increasingly become a mainstay of US communication infrastructure and is used to protect everything from video calls to emails to classified documents. For the public, encryption protects financial and medical data, enables online commerce, protects passwords and online browsing history, and provides privacy from criminals or other unauthorized users.<sup>6</sup> And as entire sectors of the economy and government work from home due to COVID-19, secure communications are essential. Where companies could create physical security and privacy measures in an office, such protections become ineffective or impractical to implement at home.

The current pandemic has made people more, not less, interested in securing their communications. The risks of insecure communications became readily apparent with white supremacists and others interrupting Zoom calls (i.e., Zoom bombing) hosted by Alcohol Anonymous and other organizations conducting sensitive and private meetings.<sup>7</sup> Due to overwhelming demand and growing security concerns, Zoom announced that it would provide its users the option to make their calls and chats end-to-end encrypted to ensure that unwanted parties could not listen to or disrupt sensitive conversations.<sup>8</sup>

Congress, too, favors using encryption. The Senate Sergeant at Arms approved the use of Signal, an encrypted messaging app, for staffers in 2017.<sup>9</sup> In the wake of COVID-19, the Sergeant at Arms' cybersecurity division advised senators not to use Zoom when convening remotely because calls on the platform were not encrypted.<sup>10</sup> But it's not just the public and Congress who rely on encryption for protection. Our national security also depends on encryption across various platforms to protect information that foreign malicious actors seek to obtain for nefarious ends. And undermining encryption could have grave implications for our national security.

## **What Is The Threat From Foreign Actors?**

In the context of encryption, the threat from foreign actors is three-fold:

1. The reliance on cyberattacks to find vulnerabilities in our systems to access national security information;
2. The transport layer on which our personal and commercial information travels is vulnerable to foreign interference; and
3. The supply chain of encryption devices may be controlled by foreign players.

First, foreign actors are constantly trying to gain access to sensitive US information on both encrypted and unencrypted channels. The hack of the Office of Personnel Management files by Chinese intelligence services in 2015<sup>11</sup> and the earlier hack of the US military's classified computer networks by Russian intelligence<sup>12</sup> shows a constant effort by foreign actors to gain access to US information. If companies are forced to create a backdoor for law enforcement purposes (explained in further detail below), they and law enforcement cannot prevent foreign actors from exploiting the same backdoor—now a vulnerability—to steal information.

Second, even when data is encrypted, it could travel across devices and platforms controlled by foreign actors. A message between Americans could be sent from, received on, or travel through equipment produced by companies like Huawei, which has close ties to Chinese intelligence and the People's Liberation Army,<sup>13</sup> which is inherently vulnerable to compromise. While encrypted communications sent over such a network are protected from unauthorized interception, unencrypted communications would be readable to anyone with access to that network. Worse, providing a system of encryption that has a built-in vulnerability

gives users the illusion that their communications are secure when, in actuality, they are not.

Finally, even when devices are made by trusted companies, they may still be reliant on supply chains that are controlled by adversarial nations. Given the globalized production of products such as internet routers, cellphones, and servers, foreign actors have multiple entry points to compromise a system. The security of the information in this environment is all the more important. If the United States adopts policies that mandate creating a vulnerability for encryption of platforms or devices, foreign or other malicious actors can more easily take advantage of the weakness. In sum, the threat from foreign actors is multi-faceted and encryption alone cannot resolve every vulnerability or threat. But weakened encryption represents the removal of a critical national security tool that is foundational to the operations of agencies like the Department of Defense (DOD).

## **What Encryption Protects For National Security**

DOD has increasingly incorporated encrypted devices into their operations to secure national security information. These services protect data in obvious scenarios, like the communication of classified materials. But DOD, and the women and men in our armed services, also rely on encryption to protect things like troop communications, information about troop movements, and unclassified but sensitive military research and technology shared with US contractors.

Secured buildings and online networks, such as Sensitive Compartmented Information Facilities (SCIFs) and the Department of Defense Information Network (DODIN), exist to preserve the physical and electronic security of classified materials. But not all communications occur within these environments. Federal agencies deal with thousands of contractors to assist in national security missions, but who may not be using secure and encrypted systems when handling sensitive information. For example, foreign adversaries have repeatedly targeted and breached military contractors and stolen intellectual property related to the F-35 program<sup>14</sup> and hundreds of gigabytes of sensitive submarine information.<sup>15</sup> If the data was encrypted, it would have rendered the stolen materials unusable or at least required the bad actors to launch attacks “that are more difficult and costly to execute” to gain access to the key to decrypt the data.<sup>16</sup> Further emphasizing the importance of encryption to national security, DOD’s chief information officer wrote a letter in 2019 to Congress explaining that “[t]he Department believes maintaining a domestic climate for state of the art security and encryption is critical to the protection of national security.”<sup>17</sup> Translating this letter into action, components of DOD have since encouraged members of the armed forces to use encrypted messaging apps like Signal to secure their communications and ensure their safety while deployed overseas.<sup>18</sup>

Not only does DOD protect its communications (or data in motion), but DOD has also taken a number of steps to protect its stored data (or data at rest). As was raised at a recent tech CEO hearing, DOD recognizes the need to protect cloud-based information and has contracted with Google to build security and app management tools for the Department's move to the cloud.<sup>19</sup> Similarly, DOD requires authentication and encryption for wireless access to data and encryption of information stored on mobile devices and computing platforms, which are commercially-provided.<sup>20</sup>

DOD, like everyone else, has come to rely on specifically designed encryption systems as well as commercially-provided encryption. Indeed, the National Institute of Standards and Technology (NIST) recommends that any sensitive data residing within the owner's domain "must be protected" and specifically recommends adoption of "data encryption schemes."<sup>21</sup>

But it is impractical and insecure for commercial vendors on which DOD relies to create secure platforms for national security agencies and not for everyone else. DOD cannot invent or assure unique access to the mathematical equations on which encryption rely. Additionally, US government experience with specially-designed legacy programs makes it harder to transition away from those programs to newer and more secure solutions, as evidenced by the CIA's decades-long reliance on Lotus Notes for email services<sup>22</sup> or the nuclear enterprise's use of 1970s floppy disk technology well into the 2010s.<sup>23</sup>

Ultimately, creating a vulnerability in commercial products could have serious national security effects, while also undermining the benefits the general public receives.

## What Law Enforcement Wants

Attorney General Barr joins a long line of law enforcement officials who have attempted to persuade Congress to require companies to provide exceptional access to their encrypted products and services. These calls began in the Clinton administration, and have been echoed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) officials in every administration since. Law enforcement officials point to instances or types of cases where they have had difficulty gaining access to encrypted communications that purportedly stymied their investigations.

With encryption devices readily available to anyone, criminals also use them to hide communications and acts, causing law enforcement to struggle to decrypt investigation-related information (commonly referred to as the "going dark" challenge). In response, law enforcement agencies have argued that encryption is a significant threat that enables malicious actors to commit their crimes or acts, and that law enforcement is unable to access information to effectively stop or prosecute them.<sup>24</sup> In a recent example, DOJ claimed an iPhone's encryption hindered its investigation into the 2019 shooting at the naval air station in Pensacola when they were trying to assess the shooter's motives. Five months

after the incident, DOJ and the FBI were able to circumvent the encryption on the phone through an undisclosed method and found that there was coordination between the shooter and an Al-Qaeda affiliate.<sup>25</sup>

DOJ and other agencies have used Pensacola and other cases as evidence for why they need “extraordinary access” or “backdoor access” to encrypted information, claiming that encryption is undermining national security. This argument is nearly 30 years old. Backdoor proponents argued for the deployment of the infamous “Clipper Chip” in 1993 to provide law enforcement with a backdoor to encrypted messages.<sup>26</sup> Today, DOJ and FBI vilify companies that offer encryption services. In 2015, when the FBI could not readily access information on the iPhones of the San Bernardino terrorists, the government pursued legal actions against Apple claiming that the company was not complying with orders to decrypt data on the phones.<sup>27</sup> The FBI Inspector General would later release a report concluding that the FBI’s litigation was unwarranted and improper.<sup>28</sup> In 2018, FBI Director Chris Wray claimed that investigators were locked out of nearly 7,800 devices they had legally obtained because of encryption protections.<sup>29</sup> Internal metrics, however, revealed that the number was closer to 1,000 to 2,000 devices, raising questions that FBI leadership was intentionally overinflating the problem posed by encryption.<sup>30</sup> Despite overstating the scope of the issue, DOJ echoed this claim again in early 2020 when Attorney General Barr criticized Apple for refusing to assist in cracking the Pensacola shooter’s phone to obtain relevant information for the investigation (Apple claims to have legally complied with all requests).<sup>31</sup> He would go on to say, “Our national security cannot remain in the hands of big corporations who put dollars over lawful access and public safety,” and called for a “legislative solution.”<sup>32</sup>

DOJ undermines its stated justifications for a legislative fix to solve its encryption challenges by the actions it has taken and the laws at its disposal to hold private companies accountable. In both Pensacola and San Bernardino, the FBI used techniques to crack the encryption without the assistance of Apple or a built-in backdoor.<sup>33</sup> Similarly, DOJ Inspector General investigations have suggested that while senior leadership may not be aware of existing capabilities to unlock encrypted phones, the officials in charge of this technology have far greater ability to circumvent encryption than the FBI or DOJ leadership publicly disclose.<sup>34</sup> Lastly, DOJ and others point to pedophiles using encryption services to exchange and view child sexual abuse material (CSAM) as a core reason why there needs to be built-in backdoors. What they fail to mention, however, is that current law requires online companies to report this type of material and can be held liable if they fail to do so.<sup>35</sup> Specifically, federal law (18 U.S.C. §§ 2251-2260A) requires that providers must report CSAM when they discover it and preserve it or risk substantial penalties if they fail to comply.<sup>36</sup> Notably, 45 million CSAM photos and videos were submitted in 2018, but DOJ struggles to manage the growing caseload.<sup>37</sup>

DOJ has made broad claims about the importance of backdoors, but these claims contain serious and lingering questions about whether backdoors are truly

necessary. To highlight this reality, former FBI General Counsel Jim Baker noted: “Perhaps most importantly, what many people on all sides of the debate will admit in private is that the United States has not experienced a terrorist or other attack of sufficient magnitude where encryption clearly played a key role in preventing law enforcement from thwarting it so as to change the contours of the public debate and motivate Congress to act.”<sup>38</sup>

## How Mandatory Exceptional Access Is A Vulnerability

If backdoors were introduced into encrypted systems, malicious actors will exploit those system’s vulnerabilities; steal the keys held by law enforcement, national security agencies, or companies; and move their communications to non-US platforms that are outside the reach of US law enforcement, while undermining US global influence. Attorney General Barr and other advocates of built-in backdoors either ignore or dismiss the fact that weakened encryption, at best, jeopardizes Americans’ privacy and, at worst, imperils national security.

However, in response to Barr’s call for legislation, a number of legislators recently introduced a pair of bills to weaken encryption standards for law enforcement purposes. First, a bipartisan group of senators introduced the “EARN IT Act” (S. 3398) to remove criminal and civil liability protections for technology companies at the state level if they do not remove online CSAM, even if they are unable to identify the illegal content because it was encrypted. While the bill was amended in an attempt to protect encryption, the expansive legal exposure that still exists in the bill could force providers to weaken their encryption standards or stop offering encryption altogether.<sup>39</sup> Senate Republicans have also released a second bill that directly targets encryption. The “Lawful Access to Encrypted Data Act” (S. 4051) would require large companies to build backdoors by default. It would require any company that receives an order from a court or a directive from DOJ compelling them to provide technical assistance in executing a warrant to build a backdoor to access encrypted data or communications.<sup>40</sup> But by creating the extraordinary access that DOJ seeks, these laws would, in effect, destroy US encryption by (1) weakening its overall security; (2) providing opportunities for malicious actors to access encrypted information; (3) discouraging domestic investment in and development of encryption platforms; and (4) weakening US negotiating positions internationally (discussed in the Reciprocity & Global Implications section below).

Simply put, if these bills become law, the built-in backdoors would make an encrypted system insecure. Instead of limiting the communication strictly to the sender, recipient, or holder of the data, a third party could have access to any and every communication. While this might seem similar to a wiretap, encryption backdoors are fundamentally different. In fact, the modern law establishing wiretaps, the “Communications Assistance for Law Enforcement Act of 1994” (P.L. 103-414), contains an “encryption carve out” for telecommunication carriers, therefore implicitly legalizing encryption while allowing for wiretaps to

occur (CALEA notably excludes internet service providers from wiretapping).<sup>41</sup> Encryption experts also unanimously agree that DOJ or a private company cannot ensure it is the only party with that extraordinary access.<sup>42</sup> Once a backdoor is created, it becomes a matter of time for nefarious actors to discover and exploit it. In other words, our adversaries can exploit the now built-in vulnerability or target the private companies and law enforcement and national security agencies that hold the key.

These fears are not mere speculation as malicious actors have compromised private and government institutions with weak encryption and security standards. For example, Juniper Networks announced that it had backdoors unintentionally inserted into some of its products that it distributed to multinational corporations and other businesses over a seven-year period.<sup>43</sup> The National Security Agency (NSA) developed the algorithm used for Juniper Networks' encryption, which outside encryption experts believed had a backdoor.<sup>44</sup> Though the extent of any criminal or foreign exploitation of this backdoor is still under investigation, the ongoing risk posed by a backdoor to user security is ever-present.<sup>45</sup> Similarly, DOD banned the use of fitness tracking devices for deployed troops after a private company publicly released geolocation data that compromised troop movements in "unknown and potentially sensitive sites" overseas.<sup>46</sup> While this information was not encrypted, it shows the risk to national security personnel using unencrypted commercial applications and communications systems.

If backdoors did exist with tech companies or federal law enforcement agencies holding the keys to access the data, we know that the federal government would struggle to protect the system from malicious actors. In 2017, the CIA experienced the "biggest unauthorized disclosure of classified information" in the agency's history due to "woefully lax" security measures (this incident is known as "Vault7"). As a result, the CIA shuttered intelligence operations that exploited vulnerabilities in systems.<sup>47</sup> Similarly, the Shadow Brokers, a criminal enterprise, compromised the NSA and released stolen vulnerabilities that existed in Microsoft's software. Malicious actors would later weaponize those vulnerabilities by creating the WannaCry and NotPetya ransomware,<sup>48</sup> which caused billions of dollars of damages worldwide.<sup>49</sup>

Even if companies could build secure backdoors—which by definition is impossible—and the US government employs the best cybersecurity mechanism to secure the keys to access the backdoor, non-state criminal actors and terrorists could use an encryption platform based outside of US jurisdiction. Millions of people use the encrypted messaging app Telegram instead of Apple's messenger or Facebook's WhatsApp specifically because they are not American.<sup>50</sup> Malicious actors are not exempt from this practice. ISIS, for example, has over 600 channels on Telegram and uses its encrypted messaging system for security purposes, despite relying on public channels that could undermine their security.<sup>51</sup> And when the Snowden leaks revealed that intelligence agencies were spying on Americans' communications, Al-Qaeda changed the encryption

products they used and reportedly created their own encrypted messaging system.<sup>52</sup> Those who commit cybercrime or other malicious actors that rely on encryption will not stay on platforms they know to have vulnerabilities, like in a system with mandated extraordinary access for law enforcement.

Proponents of backdoors believe that, if we give law enforcement a key, they will be able to keep it safe. The problem is that law enforcement at all levels would want a key, or indeed a collection of keys for each encryption platform subject to a backdoor requirement, from US national security agencies down to county sheriffs. The examples above reveal that, if the top echelons of national security like the CIA or NSA are unable to keep backdoors secure, it is highly unlikely that a local sheriff's department will be able to keep them safe. Experts have also found that as society has embraced encryption platforms the “damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago,” and that any “globally deployed exceptional access systems raises difficult problems about how such an environment would be governed” as a practical matter.<sup>53</sup>

If exceptional access were available to the full range of law enforcement agencies—federal, state, local, tribal—it would be nearly impossible to keep the system secure from malicious actors or foreign adversaries.

## **Reciprocity & Global Implications**

In addition to the security risks that come from creating a system that allows backdoor access, mandating such a system would also adversely impact global privacy and competitiveness, degrade global norms, and create dangerous precedents for foreign adversaries—like China and Russia—to pursue similar options. As of 2016, over 800 encryption products exist in the global marketplace, with only 300 produced in the United States. If the United States mandated lawful access, then users will undoubtedly flock to products produced in countries that do not have similar mandates, thereby weakening US companies’ competitiveness in the global economy.<sup>54</sup> Michael Hayden, the former director for the NSA and CIA, also noted that China and Russia would exploit US communication platforms knowing that there are backdoors built into them.<sup>55</sup>

Other countries may also follow suit and create their own “lawful access” mandates, leading to “a patchwork of multinational regulatory structure” and more restrictions on data transfers, which could undermine international law enforcement efforts.<sup>56</sup> The United Kingdom, for example, passed and introduced legislation that could force companies to create backdoors for law enforcement purposes.<sup>57</sup> Australia, too, passed a law in 2018 that requires platforms to provide access to encrypted communications.<sup>58</sup> And India finalized a proposal in early 2020 to require companies with more than five million users to make “traceable” any post performed on their platform, which would essentially destroy encryption.<sup>59</sup> This is a worrisome trend that would be exacerbated by a US law. Under the guise of backdoors becoming an international standard, our adversaries will no doubt create or strengthen mandates to access encrypted

communications to clamp down on their citizens and commit human rights atrocities. Having imposed mandates to require access, the United States' pleas for other countries to respect the privacy of communications within their borders would fall on deaf ears, imperiling the communications of Americans overseas, journalists, human rights and democracy advocates, and others.

## **Alternative Approaches**

When considering solutions to address crime perpetrated online, Congress should consider legislative solutions that address specific challenges for particular crimes rather than undermining the security of encryption systems that play a critical role in safeguarding our national security. In addition, Congress should use its oversight power to ensure law enforcement is collaborating with the private sector and using their resources and authorities effectively and efficiently to conduct investigations.

Some Members of Congress have already begun to explore alternative legislative solutions that do not rely on granting extraordinary access. For example, in response to the EARN IT Act, which aims to reduce CSAMs at the expense of encryption, Democratic senators introduced the “Invest in Child Safety Act” (S. 3629). This Act would significantly increase the number of personnel who work on these cases, expand funding for various agencies such as the Internet Crimes Against Children Task Forces, and create a new White House office to coordinate federal efforts.<sup>60</sup> The senators rightfully criticize DOJ’s view that weakened encryption would be a panacea to CSAM and point out that DOJ has “actually cut more than \$60 million from programs to prevent child exploitation and support victims.”<sup>61</sup> Similarly, the “Technology in Criminal Justice Act” (H.R. 5227) would also assist law enforcement’s efforts by increasing funding and improving training for law enforcement at the federal, state, and local levels in identifying, collecting, and using digital evidence that is legally available to them.<sup>62</sup> When evaluating these pieces of legislation or creating new proposals, Congress should consider the framework created by the National Academies of Science and the guidelines developed by the Carnegie Endowment for International Peace’s Encryption Working Group; organizations that sought to develop methodologies to assess legislation regarding encryption.<sup>63</sup>

While these legislative proposals do not fully resolve law enforcement’s problems, they touch on three important issues. To overcome the challenges associated with encryption, Congress should push federal law enforcement to work with private partners, bolster its cyber investigative capacities, and act on existing laws to pursue malicious actors, while preserving Americans’ privacy and US national security interests.

First, Congress should begin by understanding the actual challenges that impede public-private partnerships in conducting investigations to create nuanced legislation rather than eliminating encryption whole cloth. Despite Attorney General Barr’s assertions, private companies have been willing partners in criminal and national security matters. Apple has repeatedly provided significant

amounts of information outside of encrypted communications to assist investigators, such as in the San Bernardino and Pensacola cases.<sup>64</sup> Congress should have law enforcement build upon these relationships by considering proposals that improve these relationships, such as recommendations identified by the Center for Strategic International Studies' (CSIS) report "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," whose recommendations were largely incorporated in the "Technology in Criminal Justice Act" (mentioned above).<sup>65</sup> Among their proposals, CSIS recommends that law enforcement can benefit from more robust training on what data is legally available, the companies that can provide that information, and how to request it. The report also provides detailed recommendations on how companies can enhance their interactions with law enforcement, too.<sup>66</sup>

Second, Congress needs to look at existing law enforcement capabilities and authorities to determine if any potential benefits of extraordinary access can be satisfied through other investigative means. Law enforcement leaders like Manhattan District Attorney Cyrus Vance have noted that they do not need a backdoor mechanism to resolve investigations complicated by encryption, but that companies should "comply with warrants issued by impartial judges upon findings of probable cause."<sup>67</sup> As both the Pensacola and San Bernardino examples showed, law enforcement had the authority to obtain encrypted devices through a warrant, and with those devices in hand, circumvented the encryption on the individual devices to obtain the encrypted information. Private companies could also be encouraged to develop platform safety policies that enable their users to report abusive or illegal activity and share the relevant encrypted communications with the provider. Facebook, for example, allows users to "voluntarily provide [the company] with encrypted content," which allows them to "review and determine whether it is violating and then impose penalties and/or report the matter to law enforcement, if necessary."<sup>68</sup>

Lastly, Congress should hold federal law enforcement accountable by asking how current legal structures restrict their ability to perform criminal investigations and identify areas for improvement. As mentioned, DOJ already retains the authority to prosecute tech companies if they violate CSAM laws. DOJ has also "neglected even to write mandatory monitoring reports, nor did it appoint a senior executive-level official to lead a crackdown" on CSAM or "set goals to eliminate them."<sup>69</sup> Therefore, DOJ has existing legal authorities prosecutors could pursue and enforce to convict bad actors while preserving encryption. Further, these tangible policy solutions will greatly improve law enforcement's ability to close the cyber enforcement gap where only 3 in every 1,000 cybercrimes see an arrest.<sup>70</sup>

Reliance on extraordinary access opens national security agencies and officials to access and exploitation by malicious foreign and non-state actors. Ultimately it is the joint pursuit of alternative solutions that will both grant law enforcement the necessary resources and authority to combat cybercrime while protecting and relying on standard Fourth Amendment privacy protections. The Fourth

Amendment guarantees individual adjudication for things like a warrant, not the broad scope of access to all communications that exceptional access would grant.<sup>71</sup> These courses of action would be consistent with that constitutional protection, consistent with efforts that have demonstrated success, and consistent with protecting critical national security principles and priorities.

## Conclusion

Undoubtedly, criminals and terrorists abuse encryption platforms to stymie law enforcement efforts. Yet, these same tools are critical and fundamental parts of protecting classified materials from unauthorized disclosure. DOJ claims that allowing for exceptional access to these protected systems would not undermine their security, implicitly arguing that such access will not degrade overall national security and personal and commercial privacy. These arguments, however, fail to take account of existing lessons learned about the dangers of such access and overstate the importance of backdoors while distracting from more basic investment and attention to building capabilities to combat crime. Encryption backdoors cannot be the shortcut we pursue to tackle internet-enabled crime as the risk to national security is far too great and the upside decidedly questionable. Instead, Congress should ensure that federal agencies bolster public-private partnerships, receive the resources to pursue criminals, and hold the Executive Branch accountable to implementing existing laws, rather than seeking out a shortcut that is inconsistent with national security and civil liberty principles.

## Endnotes

---

<sup>1</sup> Encryption to protect “data in use” also exists, but this paper will only discuss encryption related to data in motion and data at rest.

<sup>2</sup> Doyle, Rachel. “The Founding Fathers Encrypted Secret Messages, Too.” *The Atlantic*, 30 Mach 2017, <https://www.theatlantic.com/science/archive/2017/03/h3llo-mr-pr3s1d3nt/521193/> Accessed 8 Jul 2020.

<sup>3</sup> “What is Encryption?” *Cloudflare*, <https://www.cloudflare.com/learning/ssl/what-is-encryption/> Accessed 8 Jul 2020.

<sup>4</sup> “What is Encryption?” *Cloudflare*, <https://www.cloudflare.com/learning/ssl/what-is-encryption/> Accessed 8 Jul 2020.

<sup>5</sup> “United States of America Cyberspace Solarium Commission Report.” *United States of America Cyberspace Solarium Commission*, March 2020 [https://drive.google.com/file/d/1ryMCIL\\_dZ3oOyjFqFkkf1oMxIXJGT4yv/view](https://drive.google.com/file/d/1ryMCIL_dZ3oOyjFqFkkf1oMxIXJGT4yv/view) Accessed 8 Jul 2020.

<sup>6</sup> At the same time, experts in encryption note that there is an upper limit to what kind of communications will be encrypted in the future as many companies that “provide communications services rely on access to user data for revenue streams and product functionality.” “Don’t Panic. Making Progress on the ‘Going Dark’

---

Debate” The Berkman Center for Internet & Society at Harvard University, 1 Feb 2016  
[https://cyber.harvard.edu/pubrelease/dont-panic/Dont\\_Panic\\_Making\\_Progress\\_on\\_Going\\_Dark\\_Debate.pdf](https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf) Accessed 8 Jul 2020

<sup>7</sup> “What is “Zoombombing” and Who is Behind It?” *Antidefamation League*, 4 May 2020  
<https://www.adl.org/blog/what-is-zoombombing-and-who-is-behind-it> Accessed 8 Jul 2020 and Paul, Kari. “Zoom releases security updates in response to ‘Zoom bombings’” *The Guardian*, 23 Apr 2020.  
<https://www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing> Accessed 8 Jul 2020; and Bindle, Katherine. “Zoombombing Harms the Alcoholics Anonymous Community.” *Wall Street Journal*, 5 Apr. 2020. <https://www.wsj.com/articles/zoombombing-harms-the-alcoholics-anonymous-community-11586091602> Accessed 8 Jul 2020.

<sup>8</sup> Yuan, Eric. “End-to-End Encryption Update.” *Zoom*, 17 Jun 2020. <https://blog.zoom.us/end-to-end-encryption-update/> Accessed 8 Jul 2020.

<sup>9</sup> Wyden, Ron. “Ron Wyden letter on Signal encrypted messaging.” Letter to The Honorable Frank Larkin, Sergeant at Arms, 9 May 2017. <https://www.documentcloud.org/documents/3723701-Ron-Wyden-letter-on-Signal-encrypted-messaging.html> Accessed 8 Jul 2020.

<sup>10</sup> Lima, Cristiano. “Internal Senate memo warns Zoom poses ‘high risk’ to privacy, security.” *Politico*, 09 Apr. 2020. <https://www.politico.com/news/2020/04/09/internal-senate-memo-warns-zoom-poses-high-risk-to-privacy-security-177347> Accessed 8 Jul 2020.

<sup>11</sup> Koerner, Brendan I. “Inside the Cyberattack That Shocked the US Government.” *Wired*, 23 Oct 2016. <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/> Accessed 8 Jul 2020.

<sup>12</sup> Mello Jr., John P. “Pentagon: Yep, We Got Hacked.” *TechNewsWorld*, 26 Aug 2010  
<https://www.technewsworld.com/story/70699.html> Accessed 8 Jul 2020.

<sup>13</sup> Doffman, Zak. “Huawei Employees Linked To China’s Military And Intelligence, Reports Claim.” *Forbes*, 6 Jul 2019. <https://www.forbes.com/sites/zakdoffman/2019/07/06/huawei-employees-linked-to-chinas-state-intelligence-agencies-report-claims/#d6c00194b244> Accessed 8 Jul 2020.

<sup>14</sup> Daniels, Jeff. “Chinese theft of sensitive US military technology is still a ‘huge problem,’ says defense analyst.” *CNBC*, 8 Nov 2017 <https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html> Accessed 8 Jul 2020 and O’Brien, Mike. “Pentagon Admits F-35 Data Theft is a ‘Major Problem’” *Institute for Defense and Government Advancement*, 20 June 2013.  
<https://www.idga.org/archived-content/news/pentagon-admits-f-35-data-theft-is-a-major-problem> Accessed 8 Jul 2020.

<sup>15</sup> Nakashima, Ellen and Sonne, Paul. “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare.” *Washington Post*, 8 Jun 2018.  
[https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1\\_story.html](https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html) Accessed 8 Jul 2020.

<sup>16</sup> “Decrypting the Encryption Debate: A Framework for Decision Makers.” *The National Academies of Sciences, Engineering, and Medicine*, 15 Feb 2018, p.2.9 <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> Accessed 8 Jul 2020.

---

<sup>17</sup> Khanna, Ro. "DOD encryption letter Khanna." Letter to the Honorable Lindsey Graham, 9 Dec 2019. <https://www.documentcloud.org/documents/6572247-DOD-encryption-letter-Khanna.html> Accessed 8 Jul 2020.

<sup>18</sup> Snow, Shawn; Rempfer, Kyle; and Myers, Meghann. "Deployed 82nd Airborne unit told to use these encrypted messaging apps on government cell phones." *Military Times*, 23 Jan 2020 <https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/> Accessed 8 Jul 2020.

<sup>19</sup> Tucker, Patrick, "What Google's New Contract Reveals about the Pentagon's Evolving Clouds." *DefenseOne*, 20 May 2020. <https://www.defenseone.com/technology/2020/05/what-googles-new-contract-reveals-about-pentagons-evolving-clouds/165524/> Accessed 1 Aug 2020.

<sup>20</sup> "Cybersecurity Maturity Model Certification Version 1.02." 18 Mar 2020. [https://www.acq.osd.mil/cmmc/docs/CMMC\\_ModelMain\\_V1.02\\_20200318.pdf](https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf).

<sup>21</sup> "General Access Control Guidance for Cloud Systems." NIST Special Publication 800-210 July 2020. <https://doi.org/10.6028/NIST.SP.800-210>.

<sup>22</sup> "NARA Proposed Disposition of CIA Non Senior Email." *National Archives*, 18 Aug 2014. <https://fas.org/sgp/news/2014/09/cia-email.pdf> Accessed 1 Aug 2020.

<sup>23</sup> Stack, Liam. "Update Complete: U.S. Nuclear Weapons No Longer Need Floppy Disks." *New York Times*, 24 Oct 2019. <https://www.nytimes.com/2019/10/24/us/nuclear-weapons-floppy-disks.html> Accessed 1 Aug 2020.

<sup>24</sup> "United States of America Cyberspace Solarium Commission Report." *United States of America Cyberspace Solarium Commission*, March 2020 [https://drive.google.com/file/d/1ryMCIL\\_dZ30OvjFqFkkf1oMxIXJGT4vv/view](https://drive.google.com/file/d/1ryMCIL_dZ30OvjFqFkkf1oMxIXJGT4vv/view) Accessed 8 Jul 2020.

<sup>25</sup> Evidence surfaced that the shooter coordinated with Al Qaeda in the Arabian Peninsula, which is a terrorist organization that largely operates out of Yemen. Shortell, David and Perez, Evan. "FBI finds al Qaeda link after breaking encryption on Pensacola attacker's iPhone." *CNN*, 18 May 2020. <https://www.cnn.com/2020/05/18/politics/pensacola-shooting-al-qaeda/index.html> Accessed 8 Jul 2020.

<sup>26</sup> Gallagher, Sean. "What the government should've learned about backdoors from the Clipper Chip." *Ars Technica*, 14 Dec 2015. <https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/> Accessed 8 Jul 2020.

<sup>27</sup> Rubin, Joel; Qually, James; and Dave, Paresh. "FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now." *Los Angeles Times*, 28 Mar 2016. <https://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html> Accessed 8 Jul 2020.

<sup>28</sup> "Civil Society Urges Another Inspector General Investigation After FBI Encryption Misrepresentations." Press Release, *New America*. 4 Jun 2018. <https://www.newamerica.org/oti/press-releases/civil-society-urges-another-inspector-general-investigation-after-fbi-encryption-misrepresentations/> Accessed 8 Jul 2020.

---

<sup>29</sup> Barrett, Devlin. "FBI repeatedly overstated encryption threat figures to Congress, public." *Washington Post*, 22 May 2018. [https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315\\_story.html](https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html) Accessed 8 Jul 2020.

<sup>30</sup> Barrett, Devlin. "FBI repeatedly overstated encryption threat figures to Congress, public." *Washington Post*, 22 May 2018. [https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315\\_story.html](https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html) Accessed 8 Jul 2020. In reviewing cases where law enforcement has sought to compel access to encryption, in many instances, the cases became moot when law enforcement was able to obtain the user password.

<sup>31</sup> Barrett, Devlin. "FBI repeatedly overstated encryption threat figures to Congress, public." *Washington Post*, 22 May 2018. [https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315\\_story.html](https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html) Accessed 8 Jul 2020.

<sup>32</sup> Marks, Joseph. "The Cybersecurity 202: Barr ramps up encryption war with Apple over Pensacola shooter's phone." *Washington Post*, 19 May 2020. <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/05/19/the-cybersecurity-202-barr-ramps-up-encryption-war-with-apple-over-pensacola-shooter-s-phone/5ec32a4188e0fa6727ffe363/> Accessed 8 Jul 2020.

<sup>33</sup> Marks, Joseph. "The Cybersecurity 202: Barr ramps up encryption war with Apple over Pensacola shooter's phone." *Washington Post*, 19 May 2020. <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/05/19/the-cybersecurity-202-barr-ramps-up-encryption-war-with-apple-over-pensacola-shooter-s-phone/5ec32a4188e0fa6727ffe363/> Accessed 8 Jul 2020.

<sup>34</sup> "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation." *US Department of Justice Office of the Inspector General*, March 2018. <https://oig.justice.gov/reports/2018/01803.pdf> Accessed 8 Jul 2020.

<sup>35</sup> Keller, Michael and Dance, Gabriel. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *New York Times*, 29 Sept. 2019. <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html>

<sup>36</sup> Pfefferkorn, Riana. "The Earn It Act: How To Ban End-To-End Encryption Without Actually Banning It." *Stanford Law School*, 30 Jan 2020. <https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> Accessed 8 Jul 2020

<sup>37</sup> While 45 million photos and videos were submitted, some may be supplemental information or repeat content/data. "Wyden, Gillibrand, Casey, Brown and Eshoo Introduce Legislation to Fight Online Child Exploitation." Press Release, *Senator Ron Wyden Office*, 06 May 2020 <https://www.wyden.senate.gov/news/press-releases/wyden-gillibrand-casey-brown-and-eshoo-introduce-legislation-to-fight-online-child-exploitation> Accessed 8 Jul 2020 and Keller, Michael and Dance, Gabriel. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *New York Times*, 29 Sept. 2019. <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> Accessed 8 Jul 2020.

<sup>38</sup> Baker, Jim. "Rethinking Encryption." *Lawfare*, 22 Oct 2019. <https://www.lawfareblog.com/rethinking-encryption> Accessed 8 Jul 2020.

<sup>39</sup> Pfefferkorn, Riana. "The Earn It Act Threatens Our Online Freedoms. New Amendments Don't Fix It." *The Center for Internet and Society at Stanford Law School*, 6 Jul 2020.

---

<https://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%20%99t-fix-it> Accessed 9 Jul 2020.

<sup>40</sup> United States Congress, Senate “Lawful Access to Encrypted Data Act.” 23 Jun 2020. <https://www.judiciary.senate.gov/imo/media/doc/S.4051%20Lawful%20Access%20to%20Encrypted%20Data%20Act.pdf> Accessed 8 Jul 2020.

<sup>41</sup> Pfefferkorn, Riana. “The Earn It Act: How To Ban End-To-End Encryption Without Actually Banning It.” *Stanford Law School*, 30 Jan 2020. <https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it> Accessed 8 Jul 2020 and Lewis, James; Zheng, Denise; and Carter, William. “The Effect of Encryption on Lawful Access to Communications and Data.” *Center for Strategic and International Studies*, 8 Feb 2017. <https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data> Accessed 8 Jul 2020.

<sup>42</sup> Hawkins, Derek. “The Cybersecurity 202: We surveyed 100 experts. A majority rejected the FBI's push for encryption back doors.” *Washington Post*, 11 June 2018. <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/11/the-cybersecurity-202-we-surveyed-100-experts-a-majority-rejected-the-fbi-s-push-for-encryption-back-doors/5b1d39eb1b326b6391af094a/>; <https://blog.cryptographengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/> Accessed 8 Jul 2020; and Stepanovich, Amie and Karanicolas, Michael. “Why An Encryption Backdoor for Just the “Good Guys” Won’t Work.” *Just Security*, 2 Mar 2018. <https://www.justsecurity.org/53316/criminalize-security-criminals-secure/> Accessed 8 Jul 2020.

<sup>43</sup> Wyden, Ron et al. “Wyden Led Bicameral Juniper Letter.” *Letter to Rami Rahim, Chief Executive Officer of Juniper Networks*, 10 June 2020. <https://www.wyden.senate.gov/imo/media/doc/061020%20Wyden%20Led%20Bicameral%20Juniper%20Letter.pdf> Accessed 8 Jul 2020.

<sup>44</sup> Wyden, Ron et al. “Wyden Led Bicameral Juniper Letter.” *Letter to Rami Rahim, Chief Executive Officer of Juniper Networks*, 10 June 2020. <https://www.wyden.senate.gov/imo/media/doc/061020%20Wyden%20Led%20Bicameral%20Juniper%20Letter.pdf> Accessed 8 Jul 2020.

<sup>45</sup> Wyden, Ron et al. “Wyden Led Bicameral Juniper Letter.” *Letter to Rami Rahim, Chief Executive Officer of Juniper Networks*, 10 June 2020. <https://www.wyden.senate.gov/imo/media/doc/061020%20Wyden%20Led%20Bicameral%20Juniper%20Letter.pdf> Accessed 8 Jul 2020.

<sup>46</sup> Shanahan, Patrick. “Use of Geo location-Capable Devices, Applications, and Services.” *US Department of Defense*, 03 Aug 2018. [https://partner-mco-archive.s3.amazonaws.com/client\\_files/1533573228.pdf](https://partner-mco-archive.s3.amazonaws.com/client_files/1533573228.pdf) Accessed 8 Jul 2020 and Sly, Liz. “U.S. soldiers are revealing sensitive and dangerous information by jogging.” *Washington Post*, 29 Jan 2018. [https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e\\_story.html](https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html) Accessed 8 Jul 2020.

<sup>47</sup> Nakashima, Ellen and Harris, Shane. “Elite CIA unit that developed hacking tools failed to secure its own systems, allowing massive leak, an internal report found.” *Washington Post*, 16 Jun 2020. [https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077\\_story.html](https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html) Accessed 8 Jul 2020.

<sup>48</sup> Schneier, Bruce. “Who Are the Shadow Brokers?” *The Atlantic*, 23 May 2017. <https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/> Accessed 8 Jul 2020

---

and Goodin, Dan. "Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak." *Ars Technica*, 05 Jul 2019. <https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/> Accessed 8 Jul 2020.

<sup>49</sup> Berr, Jonathan. "WannaCry" ransomware attack losses could reach \$4 billion." *CBS News*, 16 May 2017 <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/> Accessed 8 Jul 2020 and Nash, Kim; Castellanos, Sara; and Janofsky, Adam. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." *The Wall Street Journal*, 27 Jun 2018. <https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906> Accessed 8 Jul 2020.

<sup>50</sup> Karasz, Palko. "What Is Telegram, and Why Are Iran and Russia Trying to Ban It?" *The New York Times*, 02 May 2018. <https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html> Accessed 8 Jul 2020.

<sup>51</sup> Clifford, Bennett and Powell, Helen. "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." *The George Washington University: Program on Extremism*, June 2019 <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf> Accessed 8 Jul 2020.

<sup>52</sup> Ahlberg, Christopher. "How Al-Qaeda Uses Encryption Post-Snowden (Part 2) — New Analysis in Collaboration With ReversingLabs." *Recorded Future*, 1 Aug 2014. <https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/> Accessed 8 Jul 2020.

<sup>53</sup> Multiple Authors, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" *Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report*, 10 Jul 2015 <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf> Accessed 8 Jul 2020.

<sup>54</sup> "Decrypting the Encryption Debate: A Framework for Decision Makers." *The National Academies of Sciences, Engineering, and Medicine*, 15 Feb 2018, p.81 <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> Accessed 8 Jul 2020.

<sup>55</sup> Hayden, Michael. "Encryption Backdoors Won't Stop Crime But Will Hurt U.S. Tech." *Bloomberg*, 10 Dec 2019. <https://www.bloomberg.com/opinion/articles/2019-12-10/encryption-backdoors-won-t-stop-crime-but-will-hurt-u-s-tech> Accessed 8 Jul 2020.

<sup>56</sup> "Decrypting the Encryption Debate: A Framework for Decision Makers." *The National Academies of Sciences, Engineering, and Medicine*, 15 Feb 2018. <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> Accessed 8 Jul 2020.

<sup>57</sup> Lomas, Natasha. "Could the UK be about to break end-to-end encryption?" *Tech Crunch*, 27 May 2017. <https://techcrunch.com/2017/05/27/could-the-uk-be-about-to-break-end-to-end-encryption/> Accessed 9 July 2020.

<sup>58</sup> Stilgherrian. "The Encryption Debate in Australia." *Carnegie Endowment for International Peace*, 30 May 2019. <https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217> Accessed 9 July 2020.

<sup>59</sup> "Comments / suggestions invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018." *Government of India: Ministry of Electronics and Information Technology* <https://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines> Accessed 9 Jul 2020; and Newton, Casey. "India's proposed internet regulations

---

could threaten privacy everywhere.” *The Verge*, 14 Feb 2020.  
<https://www.theverge.com/interface/2020/2/14/21136273/india-internet-rules-encryption-privacy-messaging> Accessed 9 Jul 2020.

<sup>60</sup> “Wyden, Gillibrand, Casey, Brown and Eshoo Introduce Legislation to Fight Online Child Exploitation.” Press Release, *Senator Ron Wyden Office*, 06 May 2020. <https://www.wyden.senate.gov/news/press-releases/wyden-gillibrand-casey-brown-and-eshoo-introduce-legislation-to-fight-online-child-exploitation> Accessed 8 Jul 2020.

<sup>61</sup> “Wyden, Gillibrand, Casey, Brown and Eshoo Introduce Legislation to Fight Online Child Exploitation.” Press Release, *Senator Ron Wyden Office*, 06 May 2020. <https://www.wyden.senate.gov/news/press-releases/wyden-gillibrand-casey-brown-and-eshoo-introduce-legislation-to-fight-online-child-exploitation> Accessed 8 Jul 2020; and Keller, Michael and Dance, Gabriel. “The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?” *New York Times*, 29 Sept. 2019.  
<https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> Accessed 8 Jul 2020.

<sup>62</sup> US Congress, House. “H.R.5227 - Technology in Criminal Justice Act of 2019.” *Congress.gov*, 21 Nov. 2019. <https://www.congress.gov/bill/116th-congress/house-bill/5227/text> Accessed 8 Jul 2020.

<sup>63</sup> “Decrypting the Encryption Debate: A Framework for Decision Makers.” *The National Academies of Sciences, Engineering, and Medicine*, 15 Feb 2018. <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> Accessed 8 Jul 2020; and Encryption Working Group. “Moving the Encryption Policy Conversation Forward.” *Carnegie Endowment for International Peace*, 10 Sept. 2019. <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward> Accessed 09 Jul 2020.

<sup>64</sup> Barrett, Devlin and Zapotosky, Matt. “Pensacola shooting was an act of terrorism, attorney general says.” *Washington Post*, 13 Jan 2020. [https://www.washingtonpost.com/national-security/pensacola-shooting-was-an-act-of-terrorism-attorney-general-says/2020/01/13/34dbed8e-3629-11ea-bf30-ad313e4ec754\\_story.html](https://www.washingtonpost.com/national-security/pensacola-shooting-was-an-act-of-terrorism-attorney-general-says/2020/01/13/34dbed8e-3629-11ea-bf30-ad313e4ec754_story.html) Accessed 8 Jul 2020; and Rubin, Joel; Qually, James; and Dave, Paresh. “FBI unlocks San Bernardino shooter’s iPhone and ends legal battle with Apple, for now.” *Los Angeles Times*, 28 Mar 2016. <https://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html> Accessed 8 Jul 2020.

<sup>65</sup> Carter, William; Daskal, Jennifer; and Crumpler, William. “Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge” *Center for Strategic and International Studies*, 2018 July. [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725\\_Carter\\_DigitalEvidence.pdf?tAGR\\_DvxRdp0RspjGYNcGKTUjrGY3rN](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspjGYNcGKTUjrGY3rN) Accessed 9 Jul 2020; and US Congress, House. “H.R.5227 - Technology in Criminal Justice Act of 2019.” *Congress.gov*, 21 Nov. 2019. <https://www.congress.gov/bill/116th-congress/house-bill/5227/text> Accessed 8 Jul 2020.

<sup>66</sup> Carter, William; Daskal, Jennifer; and Crumpler, William. “Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge” *Center for Strategic and International Studies*, 2018 July. [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725\\_Carter\\_DigitalEvidence.pdf?tAGR\\_DvxRdp0RspjGYNcGKTUjrGY3rN](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspjGYNcGKTUjrGY3rN) Accessed 9 Jul 2020.

<sup>67</sup> Cyrus Vance, “Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety” 10 Dec 2019. <https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/> Accessed 8 Jul 2020.

---

<sup>68</sup> “Facebook’s Civil Rights Audit – Final Report.” 08 Jul. 2020. <https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf> Accessed 9 Jul 2020.

<sup>69</sup> Keller, Michael and Dance, Gabriel. “The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?” *New York Times*, 29 Sept 2019. <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> Accessed 8 Jul 2020.

<sup>70</sup> Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” *Third Way*, 29 Oct 2018, <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors> Accessed 9 Jul 2020.

<sup>71</sup> For more information regarding the 4<sup>th</sup> Amendment and the traditional warrant process, please see Huddle, Roger and Ashcroft, Gary. “Guide to Section 702 Reform.” *Third Way*, 28 Jul 2017. <https://www.thirdway.org/report/guide-to-section-702-reform> Accessed 8 Jul 2020.