REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON

SMARTPHONE ENCRYPTION *and* PUBLIC SAFETY

An update to the November 2018 Report

October 2019

Contents

Introduction

Since November 2015, this Office has written annual reports on the subject of smartphone encryption, following decisions by Apple and Google in 2014 to render data on their devices completely inaccessible without a passcode. The reports have documented the harmful impact these private business decisions have had on criminal investigations and criminal justice outcomes at the local, state, national, and international levels.

Our 2015 report was titled *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*.[1] After summarizing the encryption debate as it stood at the time, it explained the importance of evidence stored on smartphones; detailed how traditional investigatory methods cannot be used to unlock an encrypted device; and provided real-world examples of cases that were stymied and crimes that went unsolved as a result of these corporate decisions. It explained that, prior to Apple's 2014 announcement, there was no evidence that its devices were particularly susceptible to hacking, or that courts, when authorizing search warrants, were not properly protecting personal privacy interests as they have done for over two hundred years. The report proposed a legislative solution that would provide a uniform national approach to balancing consumer privacy concerns and criminal justice needs, free from technology-company influence.[2]

Our 2016 report further documented the growing impact of default smartphone encryption on law enforcement and criminal justice, and the gathering debate (dominated largely by the technology companies themselves) about the supposed divide between criminal justice and privacy interests.[3] It also warned that continued legislative inaction would lead to an untenable "arms race" between tech companies and law enforcement, in which device manufacturers continually adopt technological "fixes" whenever law enforcement is able to access data through an ad-hoc "workaround."[4]

Our 2017 report examined this unfolding arms race, and explained that, despite law enforcement's ability to develop workarounds, such solutions are cost-prohibitive to most prosecutors and investigators, causing unequal access to justice for crime victims across the country.[5] The 2017 report also provided examples of additional crimes—big and small—that were solved or remained unsolved depending on access to cellphone data, as well as cases

---

[1] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 18, 2015, *available at* https://www.manhattanda.org/wpcontent/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[2] *Id.* at 13.

[3] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report*, Nov. 17, 2016, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

[4] *Id.* at 7, 30.

[5] *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 2017, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf.

where individuals were exonerated of serious crimes because law enforcement was able to access encrypted cellphone evidence.[6]

Our 2018 report[7] provided an update on the number and status of encrypted, inaccessible devices; recent examples of cases where cellphone evidence was crucial; new developments in the U.S. courts; and legislative initiatives internationally. It went on to examine the current state of the arms race between law enforcement and device makers, including a chronology of the continuing efforts by Apple to engineer its devices and software in ways that would thwart law enforcement workarounds. It concluded with a discussion of the recent controversies that have plagued technology companies over their failures to protect consumer privacy, and why such developments only underscore the need for a legislative solution to the continuing encryption dispute.[8]

This 2019 report recounts further developments over the past year. First, courts in the United States are increasingly split on how to balance the complex issues of lawful access and privacy concerns. Second, despite some increasing international calls for regulatory or legislative solutions to resolve the privacy/security encryption debate, little has been done, domestically or internationally, to advance a solution. Finally, increased scrutiny of the technology sector and its impact on public and private life has continued to change the political and regulatory climate in which technology companies operate. These developments have called into further question the companies' motives in preventing law enforcement from accessing smartphone data, and the wisdom of making them the gatekeepers of lawful access to such data. We conclude by positing that this evolving landscape offers lawmakers in the United States an opportunity to re-evaluate the authority of technology companies to dictate what data is and is not accessible to law enforcement, and to address the issue through federal legislation: an outcome we have proposed since our first report in 2015.

I. Lawful Access to Smartphone Data: A 2019 Update

A. Cellphone Data Remains Critical to Establishing Guilt or Innocence

When a heavily armed assailant massacred nine people and injured twenty-seven others in Dayton, Ohio on August 4, 2019, it was understood by all that a full and thorough investigation was essential, not only to understand this latest mass shooting, but to prevent others from occurring. The investigation that unfolded naturally included interviews with eye-witnesses and individuals who were familiar with the suspect, a review of video surveillance,

---

[6] *Id.* at 3, 8–9.

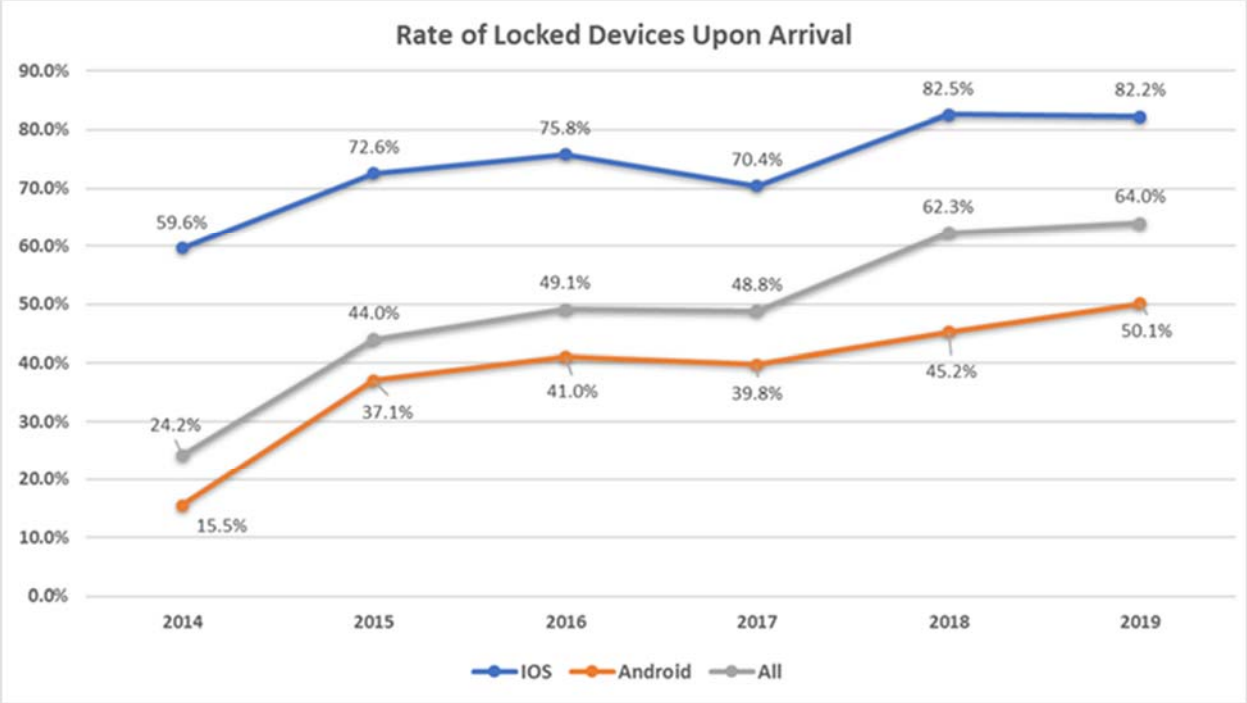
[7] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2017 Report*, Nov. 2018, *available at* https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf.

[8] *Id.* at 14–17.

an analysis of his writings, and—these days—a prompt forensic review of his personal communications devices, including his smartphones, tablets, and laptops.

Innumerable investigations of past similar crimes have taught that a suspect's personal devices can yield crucial immediate evidence of his motives, other victims, other pending dangers, and unknown accomplices. Unfortunately, however, as in countless prior investigations, the FBI—because of default smartphone encryption—has to date been unable to access one of the suspect's critical phones.[9] This inaccessibility might be shocking to some policymakers and members of the public; for law enforcement, inaccessibility is the new normal.[10]

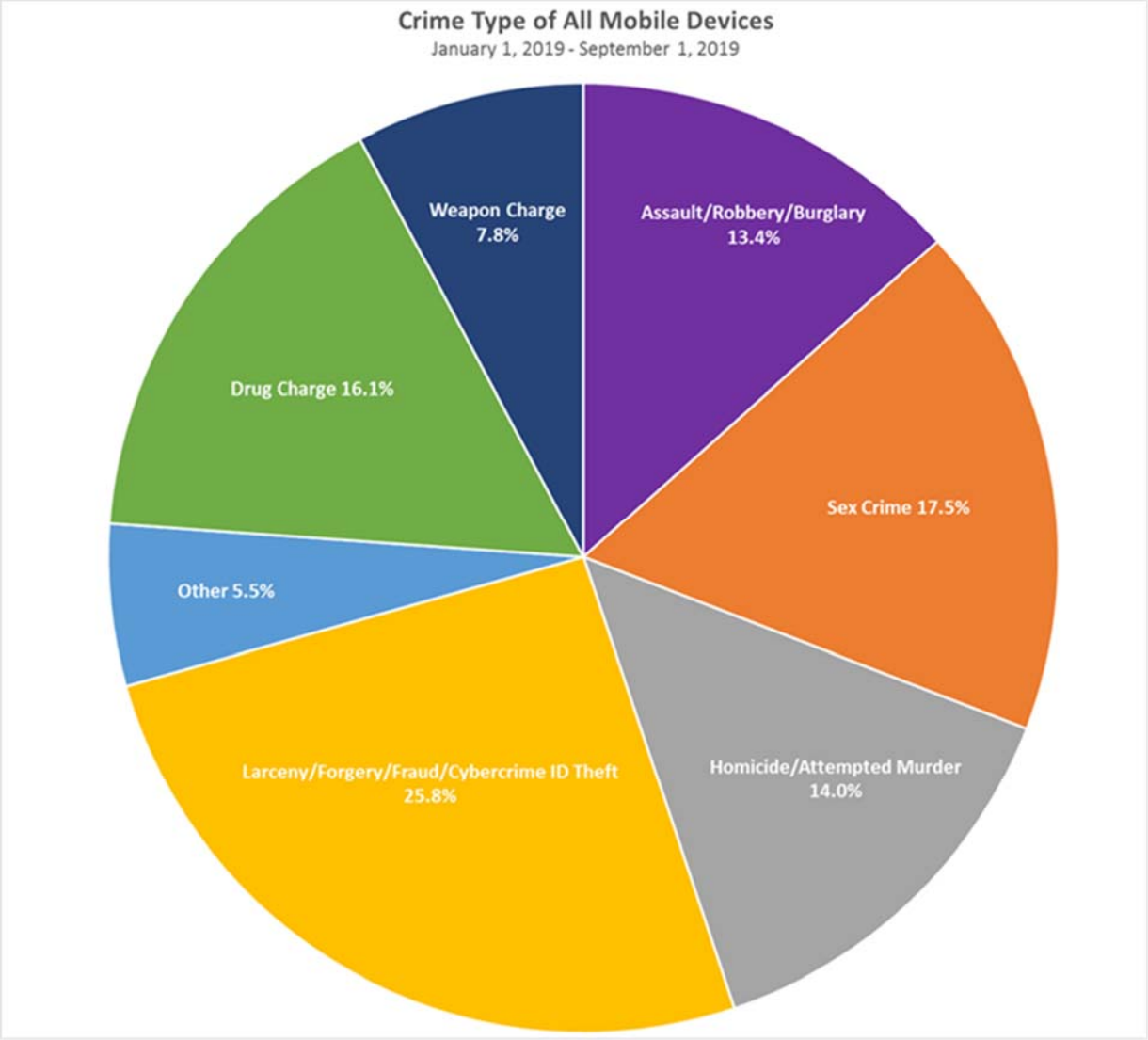
For our office and others, the number of encrypted devices containing important evidence remains high, with the trend of inaccessibility increasing each year. As the below chart indicates, the percentage of encrypted Apple devices arriving at our office has increased significantly over the past five years, from 59.6% in 2014 to 82.2% in 2019.



[9] Scott Wong & Harper Neidig, *FBI Tells Lawmakers it Can't Access Dayton Gunman's Phone*, The Hill, Aug. 8, 2019, *available at* https://thehill.com/homenews/administration/456742-fbi-tells-lawmakers-it-cant-access-phone-of-dayton-gunman.

[10] Law enforcement was similarly blocked from accessing the gunman's iPhone following the mass shooting in Sutherland Springs, Texas in November 2017. *See* Michael Marks, *Why Can't Apple Unlock the Sutherland Shooter's Phone?*, Tex. Standard, Nov. 21, 2017, *available at* https://www.texasstandard.org/stories/why-cant-apple-unlock-the-sutherland-springs-shooters-phone/.

This increase has had a direct impact on real-life criminal investigations, exonerations, and prosecutions in all manner of criminal cases, from identity theft to homicides, sexual offenses, and other violent crimes. The chart below depicts the breakdown of crimes for which our office has obtained a mobile device, whether encrypted or accessible, in the course of an arrest or investigation.



What follows are just a few examples of cases handled by this Office over the past year in which smartphone evidence was particularly critical.

- In one case, the defendant raped a woman, who, at the time of the assault, had an Order of Protection against the defendant. In an attempt to cover up the crime, the defendant created phony text messages to make it appear that the victim was falsely accusing him. The defendant's phone was locked and the contents in were inaccessible without the passcode. After a warrant was obtained, a digital forensic technician used a workaround to extract data from the defendant's phone, which showed that he had indeed sent the texts to himself using a fake texting app to impersonate the victim.

- In another case, a victim was kidnapped and robbed at gunpoint by several assailants. Investigators quickly identified one of the perpetrators but were unable to determine who else was involved in the crime. The forensic search of the perpetrator's cellphone led to the identification and seizure of a second perpetrator's phone. The initial search of that phone led to the discovery that numerous text messages had been exchanged among various unknown parties at or near the time of the kidnapping, but these messages had been deleted and were not viewable by investigators. After several months of using a third-party workaround, we were able to retrieve these deleted text messages, which were exchanged before, during, and after the kidnapping. Based on this new evidence, we were able to identify and charge the three other culprits in the crime.

- During an incident on a Manhattan street, a victim was slashed in the throat, causing a severe carotid artery wound. A suspect was charged with Attempted Murder and Assault. The defendant's phone was encrypted. After obtaining a warrant and after months of employing a workaround, the phone was unlocked, and we found video evidence which established that the defendant in fact did not commit the slashing.

- In a case charging the Dissemination of Indecent Material to Minors, the defendant, an eighth-grade teacher, gave several students his personal cell phone number and began having intimate and sexual conversations with them. Although the defendant has pleaded guilty to one count, it is believed that there are other unknown child victims. Our office obtained a warrant to access his phone, but, due to encryption, we have not been able to retrieve any such additional evidence.

- In another recent case, two defendants are charged with murder for shooting a man as he walked toward his home. It is believed that the killing was gang related, and that the defendants targeted the victim because of a rival gang

association. For proof of such a motive, and of the relationship between the defendants and the victim, our office obtained search warrants for both of the defendants' phones. One such phone indeed yielded evidence of a defendant's gang membership, his relationship with the other defendant, and his animosity toward some of the victim's associates. The other defendant's phone, however, remains inaccessible due to encryption, and similar evidence has thus not been developed for the second defendant.

B. An Update on Developments in the Courts

As discussed in our prior reports, federal and state courts, without legislative guidance, have been grappling with the question of whether and how law enforcement should be permitted to overcome encryption of electronic devices.[11] Additionally, the academic community has weighed in on the issue.[12] In years past, the threshold question has been whether, if law enforcement attempts to compel a suspect to enter a passcode to decrypt a device, such compulsion violates the user's Fifth Amendment privilege against self-incrimination. However, courts have recently begun to address the additional question of whether compelling the use of biometric data, such as fingerprints or an individual's face, to decrypt a device implicates the Fifth Amendment as well, as is discussed further below.[13]

Since our 2018 report, numerous state and federal courts have addressed the issue of compelled decryption, but no consensus has emerged. In fact, intermediate appellate courts within the same state have split on this issue.[14] Until the U.S. Supreme Court weighs in, it

---

[11] *2015 Report*, *supra* note 1, at 5; *2016 Report*, *supra* note 3, at 16–22; *2017 Report*, *supra* note 5, at 10–14; and *2018 Report*, *supra* note 7, at 9–11.

[12] *See, e.g.,* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Texas L. Rev. 767 (2019) (arguing that, when the government can independently verify that a suspect knows the passcode to an encrypted device, it becomes a foregone conclusion and the Fifth Amendment does not bar the government from enforcing a lawful decryption order); Laurent Sacharoff, *What Am I Really Saying When I open My Smartphone? An Response to Orin S. Kerr*, 97 Texas L. Rev. Online 63 (2019) (countering Professor Kerr, Professor Sacharoff contends that the government's independent knowledge should apply not to the suspect's knowledge of the passcode, but instead to its knowledge, with reasonable particularity, of the files that the person possess on the device in question); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 Fordham L. Rev. 203 (2018) (arguing that "the government can compel a suspect to decrypt only those files it already knows she possesses").

[13] *See In the Matter of the Search of a Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1015–17 (N.D. Cal. 2019); *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 2082709, at *1 (D. Idaho May 8, 2019), *vacated* 2019 WL 3401990 (D. Idaho July 26, 2019) (reversing the magistrate's order which had denied the government's request to compel defendant to decrypt his cellphone). In our 2018 report, we noted that biometric data, such as fingerprints or an individual's face, was generally not considered to be protected by the Fifth Amendment. *2018 Report*, *supra* note 7, at 10–11. Professor Kerr made a similar observation, stating that "[a] thumbprint is nontestimonial: the government can order a suspect to place his thumb on a fingerprint reader without triggering the [Fifth Amendment] privilege at all." Kerr, *supra* note 12, at 796.

[14] *See infra* notes 35–36 and text, describing the split between Florida appellate courts.

appears that state and federal courts around the country will continue to provide inconsistent guidance.

As described at greater length in our prior reports,[15] courts have typically addressed the question of compelled decryption by analyzing whether the "foregone conclusion" doctrine applies to an individual's knowledge of a device passcode, or—alternatively—to the government's knowledge of the contents of a device.[16] Under the foregone conclusion doctrine, if the government can demonstrate the "existence and location" of the information sought from a suspect, the Fifth Amendment does not apply, because the suspect would be "surrendering," and not testifying about, the information.[17] As noted, courts continue to split on the question of whether the government must simply prove the suspect has knowledge of a passcode, or whether the government must show that the actual contents of the device are known to the government prior to the compelled access.[18]

Recently, the Massachusetts Supreme Judicial Court, building upon its prior ruling in *Commonwealth v. Gelfgatt*,[19] held that, under article 12 of the Massachusetts Declaration of Rights, the foregone conclusion exception applies if the government proves "beyond a reasonable doubt" that a "defendant knows the password to decrypt an electronic device."[20] In the case, which involved sexual servitude, the Commonwealth, upon a search incident to the arrest of a defendant, recovered a cell phone that could only be decrypted with the entry of a passcode. The government sought an order to compel the defendant to decrypt the phone. In its ruling, the court reasoned that, to require a lesser burden of proof "would defeat the meaning and purpose of the [foregone conclusion] exception."[21] The Court ultimately

---

[15] *2015 Report*, *supra* note 1, at 5–6; *2016 Report*, *supra* note 3, at 16–18; *2017 Report*, *supra* note 5, at 10–11; *2018 Report*, *supra* note 7, at 10.

[16] For a detailed analysis of the foregone conclusion doctrine, see Professor Kerr's law review article on the subject of compelled decryption. *See* Kerr, *supra* note 12, at 773–78.

[17] *Fischer v. United States*, 425 U.S. 391, 411 (1976) (citing *In re Harris*, 221 U.S. 274, 279 [1911] [internal quotation marks omitted]).

[18] *Compare Commonwealth v. Jones*, 117 N.E.3d 702, 712–14 (Mass. 2019) (holding that the Massachusetts Declaration of Rights, the government must "prove that a defendant knows the password to decrypt an electronic device beyond a reasonable double for the foregone conclusion exception to apply"), *with In the Matter of the Search of a Residence in Oakland, California*, 354 F.Supp.3d 1010, 1016–18 (N.D. Cal. 2019) (holding that the foregone conclusion doctrine did not apply since the government "inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search" of the digital devices).

[19] 11 N.E.3d 605 (Mass. 2014).

[20] *Jones*, 117 N.E.3d 702 at 713.

[21] *Id.* Presumably due in part to the novelty of the issue, the Court invited amici to submit briefs on the question of what burden the government bears in order to establish a "foregone conclusion." *Amicus Announcements from September 2018 to August 2019*, *available at* https://www.mass.gov/info-details/amicus-announcements-from-september-2018-to-august-2019. One of the amici, Professor Kerr, argued in his brief that the appropriate standard of proof under the Fifth Amendment of the U.S. Constitution should be "clear and convincing evidence." *Id.* at 713 n.12; *see generally Commonwealth v. Jones*, *Brief of* Amicus Curiae *Professor Orin Kerr in Support of Neither Party*, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3264866 (arguing that "[t]he Court should hold that the Commonwealth must prove by clear and convincing evidence, based on a totality of the circumstances, that the subject of the order knows the password required to unlock the device").

found that the government had met its burden, reversing the trial court's decision, and entered an order compelling defendant to enter his passcode into the cell phone.[22]

As of the publication of this Report, the highest courts in three other states—Indiana, Pennsylvania, and New Jersey—have granted review of this issue.[23] As described below, the intermediate appellate courts in these states have split two to one as to whether the foregone conclusion exception applies to the individual's knowledge of the passcode or to the government's knowledge of the information it seeks on the device in question.

- The Superior Court of New Jersey, Appellate Division, applied the "reasonable particularity" standard to the government's information regarding the passcodes to a defendant's phones, not the contents of the phones themselves.[24] In that case—involving an Essex County Sheriff's officer who was part of a narcotics-trafficking network—the defendant surrendered his phones upon arrest to the Internal Affairs Department of the Sheriff's Office, but refused to consent to a search of his phones, or provide their passcodes. In affirming the lower court order compelling the defendant to disclose the passcodes, the court reasoned that, since the government had established, and defendant did not dispute, that the defendant "exercised possession, custody, or control over the[ ] devices," the foregone conclusion doctrine applied.[25] The court found the decisions in *Apple MacPro Computer*[26] and *Gelfgatt*[27] "persuasive authority for the conclusion that [a] defendant's Fifth Amendment right against self-incrimination is not violated by requiring him to disclose the passcodes for his iPhones."[28] The court made a similar ruling in a compelled passcode case in June.[29] Leave to appeal was granted by the New Jersey Supreme Court in May 2019; a date for oral argument has, of this this writing, not yet been set.

---

[22] *Jones*, 117 N.E.3d at 720.

[23] *See Seo v. State*, 109 N.E.3d 418 (Ind. Ct. App. 2018), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. Dec. 6, 2018) (the Court heard oral arguments on April 8, 2019); *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. Ct. 2017), *appeal granted* 195 A.3d 557 (Pa. 2018) (the Court heard oral arguments on May 14, 2019 on the following issue, as stated by Petitioner: "May [Petitioner] be compelled to disclose orally the memorized password to a computer over his invocation of privilege under the Fifth Amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania Constitution?"); *New Jersey v. Andrews*, 197 A.3d 200 (N.J. Super. Ct. App. Div. 2018), *leave granted*, 206 A.3d 964 (N.J. 2019) (leave was granted on May 3, 2019 and no argument date has been set; the statement of issue is: "Can a criminal defendant be compelled to disclose the passcode to his or her cellular phone?").

[24] *Andrews*, 197 A.3d at 204–05.

[25] *Id.*

[26] *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017).

[27] 11 N.E.3d 605.

[28] *Andrews*, 197 A.3d at 207 and n.1.

[29] *State v. White*, 2019 WL 2375391 (N.J. Super. Ct. App. Div. June 5, 2019) (holding that the state had presented sufficient evidence to demonstrate that defendant had knowledge of the passcodes for the hard drives and computer tower at issue).

- The Superior Court of Pennsylvania, in a matter of first impression for the court,[30] held that the state could compel a defendant to disclose the passcode for his computer since it was information that was not "beyond that which [defendant] has already acknowledged to investigating agents."[31] In that case, involving child pornography, a government agent had been communicating with the defendant and was aware of the IP address of the defendant's computer. The court, citing case law from other jurisdictions, noted that "the government's knowledge of the encrypted documents or evidence that it seeks to compel need not be exact[,]" and that in the instant case the record reflected a "high probability" that child pornography existed on the defendant's computer.[32] Oral argument in the case was heard by the Pennsylvania Supreme Court in May 2019; a decision has not yet been issued.

- The Court of Appeals of Indiana rejected the state's motion to compel a defendant to provide the passcode to her phone, concluding that the state had "not met the requirements of the foregone conclusion doctrine because it has not demonstrated that it can, with reasonable particularity, identify any files or describe where they are [on the phone]."[33] In this case, the defendant had alleged that an individual had raped her, and provided her phone to the police to do a forensic download. Instead of moving forward on the rape allegations, the police began to investigate the defendant for harassment. Upon her subsequent arrest, she possessed the same phone that she had provided to the police earlier. While admitting that it was her phone, she refused to provide the passcode to unlock her phone. The Indiana Supreme Court heard argument in April 2019; a decision has not yet been issued.

Other state intermediate appellate courts have also recently addressed the issue of compelled decryption, with similarly mixed results.[34] For example, state intermediate appellate courts in Florida are split on the issue of compelled decryption, with two courts holding that

---

[30] *Davis*, 176 A.3d at 874.

[31] *Id.* at 875–76.

[32] *Id.* at 876.

[33] *Seo*, 109 N.E.3d at 436. Notably, the court, in the body of its decision, provided a "structure" for courts of last resort to consider when addressing the issue of decryption requests from law enforcement. *Id.* at 439–40; *see id.* at 440 n.38 (imploring courts to consider the balance between privacy rights and law enforcement needs regarding encryption in a "comprehensive way as soon as possible").

[34] *Compare People v. Spicer*, 2019 IL App (3d) 170814 (Ill. App. Ct. 3d Dist. Mar. 7, 2019) (holding that the foregone conclusion exception did not apply because the state was not seeking the individual's passcode, but the information contained on the device), *and State v. Johnson*, 2019 WL 1028462 (Mo. Ct. App. Mar. 5, 2019) (holding that since the police had previously observed the defendant enter a passcode into the phone, the foregone conclusion exception applied).

the foregone conclusion doctrine applies to the files behind the encryption,[35] while another held that the state need only demonstrate, with reasonable particularity, "its knowledge of the existence of the passcode, [defendant's] control or possession of the passcode, and the self-authenticating nature of the passcode."[36]

Courts have not been any clearer when it comes to compelling the use of biometric data. Recently, two federal district courts have addressed the issue of compelling an individual to use biometric features (such as a thumbprint or facial or iris recognition) to unlock digital devices to conduct a duly authorized search. As discussed below, the courts were split, thus calling into question what was once thought a well-established rule:[37] that compelling an individual to use biometric features to unlock a device does not violate the Fifth Amendment.

In January 2019, a federal magistrate judge in the Northern District of California held[38] that the use of biometric features is testimonial, and that compelling an individual to provide his features to unlock a device would violate the Fifth Amendment.[39] In that case, the government applied for a warrant to search a residence and seize, among other items, electronic devices. The government further requested that any individual present be compelled to use biometric features to unlock any seized devices.[40] In denying the application, the court held that it violated the Fourth and Fifth Amendments: the Fourth because the application was overbroad, and the Fifth because compelling the individuals present to use their biometric features would violate their privilege against self-incrimination.[41]

The court reasoned that the "unlocking [of] a phone with a finger or thumb scan far exceeds the 'physical evidence' created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence."[42] It further noted that, even if the "Government may never be able to access the complete contents of a digital device, [that]

---

[35] *See G.A.Q.L. v. State*, 257 So.3d 1058, 1063–65 (Fla. 4th Dist. Ct. App. 2018) (noting that the "object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall"); *Pollard v. State*, 2019 WL 2528776 (Fla. 1st Dist. Ct. App. June 20, 2019) (agreeing, over a dissent, with the Fourth District "that unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images 'amount[s] to a mere fishing expedition'" (quoting *G.A.Q.L.*, 257 So.3d at 1064)).

[36] *State v. Stahl*, 206 So.3d 124, 135–37 (Fla. 2d. Dist. Ct. App. 2016).

[37] *See supra* note 13.

[38] Shortly after the decision, the government moved to vacate the magistrate's order. As of September 25, 2019, the matter is still pending in the district court. *See In the Matter of the Search of a Residence in Oakland, California*, Docket No. 19-70053 KAW (On July 29, 2019, the government forwarded a copy of the district court's decision in Idaho reversing the magistrate's order).

[39] *In the Matter of the Search of a Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1015–17 (N.D. Cal. 2019). Notably, the court's decision was not as a result of a suppression motion, but instead written subsequent to receiving the government's warrant application. *Id.* at 1013.

[40] *Id.* at 1013–14.

[41] *Id.* at 1014–15.

[42] *Id.* at 1016.

does not affect the analysis."[43] The court held that the foregone conclusion doctrine did not apply, since smartphones contain massive amounts of data that cannot be anticipated by law enforcement, and that "the Government inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search of these unknown digital devices."[44]

Similarly, a federal magistrate judge in the District of Idaho held that compelling the use of an individual's fingerprint to unlock a phone violates the Fifth Amendment.[45] In that case, subsequent to a lawful search of a residence, federal law enforcement officers found a Google phone in a bathroom. The officers then applied for an additional search warrant authorizing law enforcement to compel the occupant of the residence to press his finger to the phone to unlock the device. In the submission, the government stated that, when asked, the individual indicated that his phone was in the bathroom where the phone in fact was later recovered.[46] Although finding the underlying search of the residence was lawful, the magistrate held that the compelled use of the individual's fingerprint violated the Fourth and Fifth Amendments, reasoning that unlocking the phone with a fingerprint was testimonial, as it would communicate ownership or control over the device (in violation of the Fifth Amendment right against self-incrimination), and that the search was thus unreasonable under the Fourth Amendment.[47]

The Court, similar to the California federal district court, had *sua sponte* raised these constitutional issues with regard to the lawfulness of the warrants in question. "In sum, what the Government would characterize as innocuous is instead a potentially self-incriminating testimonial communication because it involves the compelled use of biometrics—unique to the individual—to unlock the device. The Fifth Amendment does not permit such a result."[48] The court did not address the foregone conclusion doctrine.

The government then made a motion to reverse or vacate the Idaho magistrate's Order,[49] which was granted by a district court judge.[50] The district court judge, after noting that neither the U.S. Supreme Court, nor any federal circuit, had dealt with the issue at hand,[51]

---

[43] *Id.*
[44] *Id.* at 1017–18.
[45] *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 2082709, at *1 (D. Idaho May 8, 2019).
[46] *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 3401990, at *1 (D. Idaho July 26, 2019).
[47] *Id.* at *3.
[48] *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 2082709, at *5.
[49] *See Motion to Reverse or Vacate Magistrate's Order Denying Search Warrant Application*, 2019 WL 3422134 (D. Idaho May 16, 2019).
[50] *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 3401990, at *1.
[51] *Id.* at *3 ("The compelled unlocking of digital devices using biometric means is an emerging area of law that raises both Fourth and Fifth Amendment concerns. There appears to be several decisions throughout the country that have addressed the issue in the federal district courts with mixed results.").

adopted the Government's position that the use of a fingerprint to unlock a device is not testimonial and is more akin to other compelled displays of certain physical character features.[52] At the same time, the court seemed to accept as a given that compelling the production of a device's passcode does violate the Fifth Amendment.

In short, recent cases addressing these varying encryption issues continue to provide inconsistent guidance to law enforcement, and reaffirm the conclusion that legislation is needed here.

C. An Update on Developments Internationally

As discussed in our prior reports, the debate over encryption extends across borders, and is typically framed—as in the United States—as a tradeoff between public safety and privacy. While a variety of countries continue to grapple with the question of how to respond to tech company encryption, a workable solution has yet to be reached, largely because the tech companies themselves continue to maintain their absolutist position that no form of lawful access can be reconciled with privacy concerns.

The "Five Eyes"

As noted in last year's report,[53] in 2018 the Five Country Ministerial,[54] commonly referred to as the "Five Eyes" countries, released a joint statement titled *Statement of Principles on Access to Evidence and Encryption*, which called upon technology firms to provide lawful access to encrypted data.[55] While acknowledging a shared commitment to personal rights and privacy, the statement asserted that privacy concerns are "not absolute." Citing longstanding principles that have allowed government authorities to search homes and vehicles for otherwise private information, the statement warned that, if impediments to access continue, "we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions."[56]

In the summer of 2019, the Five Eyes members held another conference in which senior ministers met to discuss ways of coordinating with the tech sector on encryption. Among the key themes was the need for international coordination in the face of emerging threats. Speaking at the conclusion of the conference, United States Attorney General William Barr noted that, "making our virtual world more secure should not come at the expense of

[52] *Id.* at *6–7 (citing various U.S. Supreme Court cases).
[53] *2018 Report*, *supra* note 7, at 12.
[54] Member states include: Australia, Canada, New Zealand, the United Kingdom, and the United States.
[55] Five Country Ministerial. 2018. "Statement of Principles on Access to Evidence and Encryption," *available at* https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf.
[56] *Id.*

making us more vulnerable in the real world."[57] Following the conference, the group released a statement reaffirming its commitment to pursuing lawful access to encrypted devices.[58]

Australia

In the wake of the Five Eyes' concerns, the latest nation to pursue a legislative measure is Australia.[59] As discussed in our last report,[60] the Australian legislature introduced a bill in 2018 that would require communications companies—under penalty of large fines—to provide assistance to law enforcement.[61] The proposal was premised on the conclusion that "increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations, . . . and detect intrusions."[62] The proposal was immediately criticized by members of the technology industry, among them prominent academic and cryptographer Bruce Schneier, who commented that it was "written by non-technologists and it's not just bad policy. In many ways, I think it's unworkable."[63]

In the past year, the criticisms have continued, but the proposed bill has been passed into law.[64] The *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill* ("AAB") now establishes a framework for both voluntary and mandatory industry assistance to Australian law enforcement and intelligence agencies that is to be triggered by a

---

[57] Home Office & The Rt. Hon. Priti Patel, *Security Summit Ends with Pledges to Tackle Emerging Threats*, July 30, 2019, *available at* https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats.

[58] Home Office. 2019, *Joint Meeting of Five Country Ministerial and Quintet of Attorneys-General: Communique, London 2019*, July 31, 2019, *available at* https://www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019.

[59] Our prior reports described legislative proposals at various stages of discussion in the United Kingdom, France, and Germany. *See 2015 Report*, *supra* note 1, at 16–17; *2016 Report*, *supra* note 3, at 27–28; *2017 Report*, *supra* note 5, at 14–17; *2018 Report*, *supra* note 7, at 12–13. It does not appear that any of these legislative proposals have substantially advanced in the past year.

[60] *See 2018 Report*, *supra* note 7, at 12–13.

[61] The Parliament of the Commonwealth of Australia. 2018, Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application%2Fpdf.

[62] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Explanatory Memorandum, House of Representatives of the Commonwealth of Australia, *available at* http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf.

[63] Rod McGuirk & Frank Bajak, *Australia Anti-Encryption Law Rushed to Passage*, AP News, Dec. 7, 2018, *available at* https://www.apnews.com/f7055883421c4082a0d8bbb1f5268a2c. Apple similarly called the bill "dangerously ambiguous." *Id.*

[64] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, *supra* note 61.

governmental notice.[65] Such notices may be issued to any entity that provides online services or communications equipment within Australia (e.g., websites, applications, and telecom companies), and may compel the recipient to undertake a number of actions ranging from removing forms of electronic protection that they themselves have applied, to installing and using certain software or equipment.[66]

Importantly, the AAB includes language that explicitly prohibits the government from requiring a company to take steps that would create a "systemic weakness or systemic vulnerability" that would jeopardize user security.[67] In other words, the law seeks to balance law enforcement needs and privacy concerns, an approach we have advocated in our prior reports. Unfortunately, this effort does not appear to have incentivized technology companies to seek such a balance.

Instead, the technology companies immediately repeated their position—consistent with what Apple has been saying since 2014—that, having given up the keys to encryption in the design of their software, they are no longer in a position to comply with any governmental requests. For example, in December 2018, Signal developer Joshua Lund published a blog post stating that the "end-to-end encrypted contents of every message and voice/video call are protected by keys that are entirely inaccessible to us."[68] Recently, Australian cloud services provider Vault Systems reported seeing an "exodus of data from Australia including physical, operational, and legal sovereignty."[69] Vault, however, acknowledged that these negative repercussions are largely due to the perceived compliance costs of the new law, even though such companies also operate in Russia and China.[70]

In other words, the reaction by many multinational tech companies appears to have been to reduce their presence in Australia, rather than comply with the new law or engage in discussion about a technological compromise.

To counter this narrative, the Australian government in August 2019 published public guidance to dispel "myths" about the new Act.[71] The publication makes clear, for example,

---

[65] Stilgherrian, *What's Actually in Australia's Encryption Laws? Everything You Need to Know*, ZDNet, Dec. 10, 2018, *available at*. https://www.zdnet.com/article/whats-actually-in-australias-encryption-laws-everything-you-need-to-know/.

[66] Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018, *supra* note 61, at 14–23.

[67] *Id.* at 84–90.

[68] Catalin Cimpanu, *Signal: We Can't Include a Backdoor in our App for the Australian Government*, ZDNet, Dec. 14, 2018, *available at* https://www.zdnet.com/article/signal-we-cant-include-a-backdoor-in-our-app-for-the-australian-government/.

[69] Chris Duckett, *Encryption Laws are Creating an Exodus of Data from Australia: Vault*, ZDNet, July 5, 2019, *accessible at* https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/.

[70] *Id.*

[71] *Assistance and Access: Common Myths and Misconceptions*, Australian Government Department of Home Affairs, *available at* https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act, last updated Sept. 16, 2019.

that the law will not "create backdoors and undermine information security."[72] To date, the AAB does not appear to have resulted in actions that have found their way into the Australian courts, and it is too early to predict what impact the new law will have on the ongoing international debate.

The European Union

Our 2017 report discussed efforts by the European Commission to encourage "a better and more structured collaboration between authorities, service providers, and other industry partners" in an effort to promote a more a coordinated approach to the technical and legal challenges posed by encryption.[73] In January 2019, Europol expanded further on this message, in a *First Report of the Observatory Function on Encryption*.[74] This new report explicitly recognizes that the current debate about encryption has become too polarized, with tech companies unnecessarily framing the issue as a "zero-sum game," in which any tool that provides lawful access to law enforcement will necessarily compromise user privacy.[75] To break this logjam, the EU advocates "targeted approaches" to the development of new investigative tools that are "proportionate to the crime that was committed."[76] This approach is consistent with the European Commission's prior commitment to research "functional encryption:"[77] technologies that would change the way data is encrypted in the first place, to allow law enforcement to gain selective access to data in certain circumstances, instead of granting "all or nothing" law enforcement access to a device.

Again, these discussions are at an early stage, and where they lead remains to be seen. But the concept is consistent with what our office has been advocating since our first report. Ideally, technology companies will abandon their steadfast refusal to discuss solutions and instead participate in an effort to come up with a balanced technical and legal outcome. If they do not, as discussed below, the changing political and regulatory landscape may well compel a legislative result.

---

[72] *Id.*

[73] *2017 Report*, *supra* note 5, at 15.

[74] Europol, Eurojust, & European Cybercrime Centre, *First Report of the Observatory Function on Encryption*, Jan. 11, 2019, *available at* http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/First%20report%20of%20the%20observatory%20function%20on%20encryption%20(joint%20Europol-Eurojust%20report%20-%20January%202019)/2019-01_Joint-EP-EJ-Report_Observatory-Function-on-Encryption_EN.pdf.

[75] *Id.*

[76] European Commission. 2018. *Communication from the Commission to the European Parliament, the European Council and the Council*. Strasbourg, April 17, at 33, *available at* https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180317-progress-report-14-towards-effective-and-genuine-security-union_en.pdf.

[77] *Functional Encryption Technologies*, European Commission, *available* at https://cordis.europa.eu/project/rcn/213111/factsheet/en, last updated Sept. 6, 2019.

II. The Changing Political and Regulatory Climate

Our 2018 report recounted how a number of high-profile controversies in the prior year had begun to call into public question the wisdom of relying on big technology companies to be the sole arbiters of whether to make their customers' data available pursuant to legal process.[78] At the time, scandals like the one involving Facebook and Cambridge Analytica (in which a British political consulting firm was able to gain access to the private data of 87 million Facebook users and sell it to political campaigns) cast light on the fact that such companies naturally make their decisions based not on good public policy, but on their economic self-interest.[79]

One developing story in last year's report involved Google's Project Dragonfly, a search engine to be launched in China that was designed by Google to comply with Chinese government censorship policies. The product was to restrict website and search results relating to subjects like human rights, democracy, peaceful protest, and religion. The planned launch provoked immediate outcry among legislators and the public, in which Google was accused of pursuing profits (China is Google's second-largest market) in a manner that would censor free speech and facilitate human rights abuses by an autocratic regime.[80] In July of 2019, after months of continuing criticism, Google terminated its Project Dragonfly project, but refused to commit that it would not move forward with a different censored product in China in the future.[81]

In the meantime, American legislators and others in the past year have begun to express serious concerns about the fundamental business model of many technology companies, in which they harvest private user data—in ways that are little understood by the users—in order to sell the information at great profit to advertisers and others. At its core, the concern is that technology companies promote their products as "free," but in reality they track everything their users do online and market that valuable information to third parties, without compensation to, or consent from, the users themselves.[82] As Missouri Senator Josh Hawley has stated, "[w]hen a big tech company says its product is free, consumers are the ones being sold."[83] To address this concern, Senator Hawley and Senator Mark Warner of Virginia introduced bipartisan legislation in June 2019 that would require tech companies to disclose to consumers and regulators the types of data they collect, and provide users with assessments

---

[78] *2018 Report*, *supra* note 7, at 14–18.
[79] *Id.*
[80] *Id.* at 15–17.
[81] Jeb Su, *Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine*, Forbes, July 19, 2019, *available at* https://www.forbes.com/sites/jeanbaptiste/2019/07/19/confirmed-google-terminated-project-dragonfly-its-censored-chinese-search-engine/#12cad9467e84.
[82] Associated Press, *What's Your Data Worth to Big Tech? Bill Would Compel Answer*, CBS Chicago, June 24, 2019, *available at* https://chicago.cbslocal.com/2019/06/24/worth-of-data-bill-clarifies-answer/.
[83] *Id.*

of the data's value to the company.[84] Others have proposed taxing the companies' revenue from the sale of targeted digital ads as a means to change the economic model.[85]

Other concerns have continued to unfold. For example, the expanding antitrust investigations of "Big Tech" reflect the view that such companies have too much control over the marketplace, including their customers' personal data and decision making.[86] Facebook's recent announcement of its new digital currency proposal Libra was met with congressional and industry dismay: it has been reported that Libra's partners "are hesitant to associate themselves too closely with the Libra project," due to "Facebook's issues with regulators around the world, the company's shaky track record on privacy, and how it treats corporate partners, and the uncertain legality of cryptocurrencies."[87] And Google-owned YouTube recently agreed to pay a $170 million fine and provide new protections for children after it was alleged that it illegally collected children's data to sell ads for products.[88, 89]

In short, these companies that were once perceived as "young, freewheeling and rebellious," and as "quirky 'startups,'"[90] are now corporate behemoths facing suspicion and criticism from both sides of the political aisle:

---

[84] *Id.*

[85] *See* Paul Romer, *A Tax That Could Fix Big Tech*, N.Y. Times Opinion, May 6, 2019, *available at* https://www.nytimes.com/2019/05/06/opinion/tax-facebook-google.html; Press Release, Jones Day, *French Parliament Passes GAFA Tax*, July 22, 2019, *available at* https://www.jdsupra.com/legalnews/french-parliament-passes-gafa-tax-77494/; *Amazon to Pass Cost of France's New Digital Tax onto French Consumers*, RFI, Aug. 2, 2019, *available at* http://en.rfi.fr/france/20190802-amazon-pass-cost-frances-new-digital-tax-french-clients.

[86] *See* Steve Lohr, *House Antitrust Panel Seeks Documents from 4 Big Tech Firms*, N.Y. Times, Sept. 13, 2019, *available at* https://www.nytimes.com/2019/09/13/technology/amazon-apple-facebook-google-antitrust.html?auth=login-email&login=email; Matt O'Brien, *Big Tech Faces a New Set of Foes: Nearly All 50 States*, AP News, Sept. 10, 2019, *available at* https://www.apnews.com/8fae76b9b37d473caff2c94a59029a57.

[87] *See* Nathaniel Popper, *Regulators Have Doubts About Facebook Cryptocurrency. So Do Its Partners.*, N.Y. Times, June 25, 2019, *available at* https://www.nytimes.com/2019/06/25/technology/facebook-libra-cryptocurrency.html; Zachary Warmbrodt, *Facebook Rebuffs Maxine Waters on Cryptocurrency Delay*, Politico, July 17, 2019, *available at* https://www.politico.com/story/2019/07/17/facebook-rebuffs-waters-libra-delay-1596870.

[88] Rob Copeland, *YouTube Agrees to $170 Million Fine, New Protections for Children*, Wall St. J., Sept. 4, 2019, *available at* https://www.wsj.com/articles/youtubes-ftc-penalty-exposes-divisions-among-federal-regulators-11567602817?mod=article_inline.

[89] Still other critics have pointed out that technology companies are more willing to invest money in legal fees and lobbying costs than to spend time discussing these emerging concerns. For example, it was reported that Apple's lobbying spending in the U.S. grew from $4 million in 2014 to $7 million in 2017, and that "Apple, Amazon, Facebook and Google cumulatively racked up a roughly $50 million tab fighting off President Donald Trump and an onslaught of new federal regulations last year—a reflection that the tech industry is increasingly under political siege in the nation's capital." Tony Romm, *Apple, Amazon, Facebook and Google Spent Nearly $50 Million—a Record—to Influence the U.S. Government in 2017*, Vox, Jan. 23, 2018, *available at* https://www.vox.com/2018/1/23/16919424/apple-amazon-facebook-google-uber-trump-white-house-lobbying-immigration-russia; *Apple Inc*, Center for Responsive Politics, *available at* https://www.opensecrets.org/lobby/clientsum.php?id=D000021754, last visited Sept. 24, 2019.

[90] Will Oremus, *Big Tobacco. Big Pharma. Big Tech?*, Slate, Nov. 17, 2017, *available at* https://slate.com/technology/2017/11/how-silicon-valley-became-big-tech.html.

- "Facebook has said, 'Just trust us,' . . . And every time Americans trust you, they seem to get burned." – Senator Sherrod Brown (D-Ohio).[91]

- "I don't trust you guys." – Senator Martha McSally (R-Arizona) (referring to Facebook).[92]

- "Clearly, our trust and patience in your company and your monopoly has run out[.]" – Senator Josh Hawley (R-Missouri) (regarding Google).[93]

- "You can be an umpire or you can own teams, but you can't be an umpire and own one of the teams that's in the game." – Senator Elizabeth Warren (D-Massachusetts) (regarding "Big Tech").[94]

- "We cannot allow giant companies to assert their power over critical public infrastructure." – Senator Mike Crapo (R-Idaho) (regarding Facebook).[95]

This bipartisan outcry for regulation of technology companies, including in the privacy sphere, only underscores the need for regulation in the area of data encryption. Attorney General William Barr made this point in the Keynote Address at the International Conference on Cyber Security in July 2019.[96] Highlighting that it is service providers, device manufactures, and application developers—not lawmakers—who control how private information is used, he stated that, "as a result, law enforcement agencies are increasingly prevented from accessing . . . evidence essential to detecting and investigating crimes."[97] Barr acknowledged that cybercriminals and hackers pose threats, but emphasized that we also face threats from violent criminals, terrorists, and predators, all of whom live in the digital age. He cautioned, "[w]hile we should not hesitate to deploy encryption to protect ourselves from cybercriminals, this should not be done in a way that eviscerates society's ability to defend itself against other types of criminal threats."[98]

---

[91] Steve Lohr, Mike Isaac & Nathaniel Popper, *Tech Hearings: Congress Unites to Take Aim at Amazon, Apple, Facebook and Google*, N.Y. Times, July 16, 2019, *available at* https://www.nytimes.com/2019/07/16/technology/big-tech-antitrust-hearing.html.

[92] *Id.*

[93] *Id.*

[94] Nellie Bowles, *Elizabeth Warren Sticks Her Message in Big Tech's Face*, N.Y. Times, June 3, 2019, *available at* https://www.nytimes.com/2019/06/03/technology/elizabeth-warren-big-tech-break-up.html.

[95] David Dayen, *A Week of Reckoning for Big Tech*, Am. Prospect, July 16, 2019, *available at* https://prospect.org/article/week-reckoning-big-tech.

[96] Press Release, U.S. Dept. of Just., *Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security*, July 23, 2019, *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

[97] *Id.*

[98] *Id.*

Conclusion

In short, Big Tech should not be the entity to regulate Big Tech. Rather, Congress, comprised of democratically elected officials, "must determine the balance in our society between personal privacy and public safety."[99]

[99] Cyrus R. Vance Jr., Jackie Lacey & Bonnie Dumanis, *Congress Can Put iPhones Back Within Reach of Law Enforcement*, L.A. Times Opinion, May 11, 2016, *available at* https://www.latimes.com/opinion/op-ed/la-oe-vance-congress-act-on-iphones-20160511-story.html.

The New York County District Attorney's Office
One Hogan Place, New York, NY 10013

www.manhattanda.org