Cyrus Vance, Jr.

Manhattan District Attorney

Cyrus Vance, Jr. has been Manhattan District Attorney since 2010. D.A. Vance's achievements include takedowns of major gun traffickers and international cybercrime operations, the first-ever convictions on New York State terror charges, and the allocation of $35 million to help end the national backlog of untested rape kits. He has reduced unnecessary incarceration and ended the prosecution of thousands of low-level, nonviolent offenses annually, most recently ending the criminal prosecution of marijuana possession and smoking, as well as subway turnstile-jumping.

D.A. Vance is the co-founder and co-chair of Prosecutors Against Gun Violence, and co-founder of the Global Cyber Alliance.

Draft Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.
Before the Commission on Law Enforcement and the Administration of Justice

Final Version to be Submitted at Later Date

April 15, 2020

Good afternoon Chairman Keith, Vice Chairman Sullivan, and Commissioners of the President's Commission on Law Enforcement and the Administration of Justice. Before I begin my remarks, I want to wish all of you, your Commission's staff, and your personal staff in your home jurisdictions the very best during this extremely difficult time.

On behalf of my Office and our partners in state and local law enforcement, I commend this Commission for holding today's important virtual panel on technology issues encountered by law enforcement. I thank you for the opportunity to testify on encryption and lawful access – a vital issue of local, state, and national public safety.

This past December, I testified before the U.S. Senate Judiciary Committee[1] on the exigent need for federal legislation ensuring lawful access to encrypted evidence from tech giants such as Apple, Google, and Facebook. Based on this testimony, my Office subsequently met with senior staff from Google and Apple in February to discuss potential solutions. To date, no substantive changes have resulted from these meetings, and I remain convinced that federal legislation is required to achieve lawful access.

When addressing tech issues faced by law enforcement, the single most important criminal justice challenge in the last ten years is, in my opinion, the use of mobile devices by bad actors to plan, execute, and communicate about crimes. Just as ordinary citizens rely on digital communication, so do people involved in terrorism, cyber fraud, murder, rape, robbery, and child sexual assault.

For this reason, lawful, court-ordered access to these communications has become essential for us to prevent crime, to hold people accused of crimes accountable, and to exonerate the innocent.

---

[1] Written Testimony of the New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary. "Smartphone Encryption and Public Safety." 10 December 2019. https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/

Until the fall of 2014, Apple and Google routinely provided law enforcement access to their mobile phones when they received a court-ordered search warrant. That changed when they rolled out their first mobile operating systems that, by design, often make the contents of smartphones completely inaccessible. In doing so, Apple and Google effectively upended centuries of American jurisprudence holding that nobody's property is beyond the reach of a court-ordered search warrant.

In 2014, my Office stood in the vanguard of American law enforcement sounding the alarm about the dangers of default smartphone encryption.[2] In subsequent years, I have delivered this call in testimony to the U.S. House and Senate, and joined with law enforcement leaders in the U.S.[3] and Europe[4] in op-eds that explained the public safety import of this issue. My Office has also published five annual reports on Smartphone Encryption and Public Safety providing unique and valuable data and analysis on this topic.[5]

Apple and Google, meanwhile, have framed this issue as an either/or proposition. Either we can have user privacy or lawful access, but we can't have both, they say. And they've been successful in propagating this message, even though it's not true.

My Office is not anti-encryption. Far from it. We routinely use encryption in the course of our daily work, whether in guarding our city's critical infrastructure against cybersecurity threats or soliciting tips on crimes against immigrant New Yorkers, and we recognize its value in our society and across the world. That does not mean encrypted material should be beyond the law when a judge signs a search warrant – especially when we're talking about evidence tied to a child sex abuse case or a potential terrorist attack.

Apple and Google have maintained their absolutist position that no form of lawful access can be reconciled with privacy concerns. Yet they have not demonstrated to law enforcement leaders what, if any, damaging effects to user privacy their pre-2014 cooperation with law

---

[2] Vance Jr., Cyrus R. "Apple and Google threaten public safety with default smartphone encryption." *The Washington Post*, 26 September 2014. https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html

[3] Vance Jr., Cyrus R., Jackie Lacey and Bonnie Dumanis. "Op-Ed: Congress can put iPhones back within reach of law enforcement." *Los Angeles Times*, 11 May 2016. https://www.latimes.com/opinion/op-ed/la-oe-vance-congress-act-on-iphones-20160511-story.html

[4] Vance Jr., Cyrus R., François Molins, Adrian Leppard and Javier Zaragoza. "When Phone Encryption Blocks Justice." *The New York Times*. 11 August 2015. https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html

[5] Manhattan District Attorney's Office. *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2018 Report.* October 2019. https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf. See also Manhattan District Attorney's Office 2018 Report, https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf; 2017 Report, https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf; 2016 Report, https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and 2015 Report, https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf

enforcement caused.[6] Further, they have decided for their own private business interests that the Fourth Amendment grants a right, not just to privacy, but to anonymity. This is wrong, and it upends the careful balance our Constitution strikes between privacy and public safety interests.

I. HOW SMARTPHONE ENCRYPTION AFFECTS PROSECUTORS AND VICTIMS OF CRIME

So how has default smartphone encryption affected law enforcement and crime victims? Let me answer these questions with two brief examples from my own Office.

The first involves child sexual abuse. A babysitter at a local church in Manhattan was identified as having shared images of child sexual assault online. Pursuant to a search warrant, his encrypted mobile phone and other devices were seized. Over time, we opened the devices using technology from a paid consultant. We then discovered the suspect was, not only sharing images of child sexual assault, but sexually abusing children himself, and recording the abuse as well. Based on this evidence, we charged him and a jury convicted him of predatory sexual assault of children.[7] He was subsequently sentenced to 100 years to life in prison.[8]

In the second example, we were not so lucky. My Office was investigating a case of sex trafficking, and obtained an encrypted phone from a suspect who was incarcerated on a different case. In a recorded telephone call from prison, the suspect told an accomplice that he hoped his phone had the newest encrypted operating system.

The inmate said to his friend, "Apple and Google came out with these softwares that can no longer be [un]encrypted by the police … [i]f our phone[s are] running on iOS8 software, they can't open my phone. That may be [a] gift from God."

In fact, we were never able to view the contents of his phone because of this gift to sex traffickers that came, not from God, but from Apple. As a result, our investigation of sex trafficking was blocked by encryption.

---

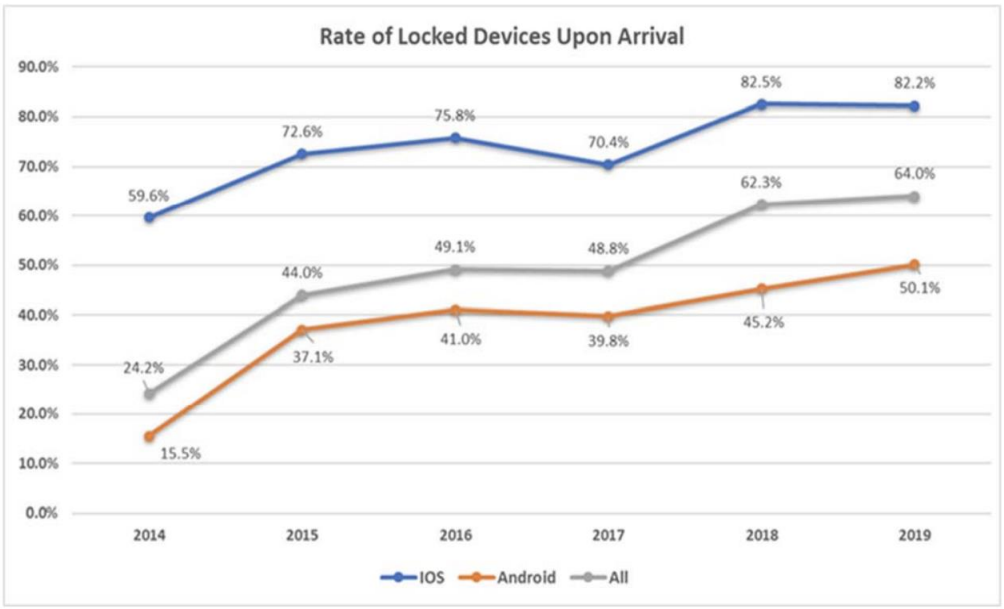
[6] Bruce Sewell, Senior Vice President and General Counsel for Apple, Inc., Responses to Questions for the Record, "The Encryption Tightrope: Balancing Americans' Security and Privacy," at p. 2. Question 6(b)(1). U.S. House Committee on the Judiciary, 1 March 2016. Was the technology you possessed to decrypt these phones ever compromised? Answer: The process Apple used to extract data from locked iPhones running iOS7 or earlier operating systems was not, to our knowledge, compromised.

[7] Manhattan District Attorney's Office. "DA Vance: Babysitter Convicted at Trial for Sexually Assaulting Two Children. 28 November 2017. https://www.manhattanda.org/da-vance-babysitter-convicted-trial-sexually-assaulting-two-children/

[8] Siegel, Jefferson and Shayna Jacobs. "NYC babysitter gets 100 years to life for raping two kids, recording the assaults." New York Daily News, 23 March 2018. https://www.nydailynews.com/new-york/nyc-crime/manhattan-babysitter-100-years-life-raping-2-kids-article-1.3893108

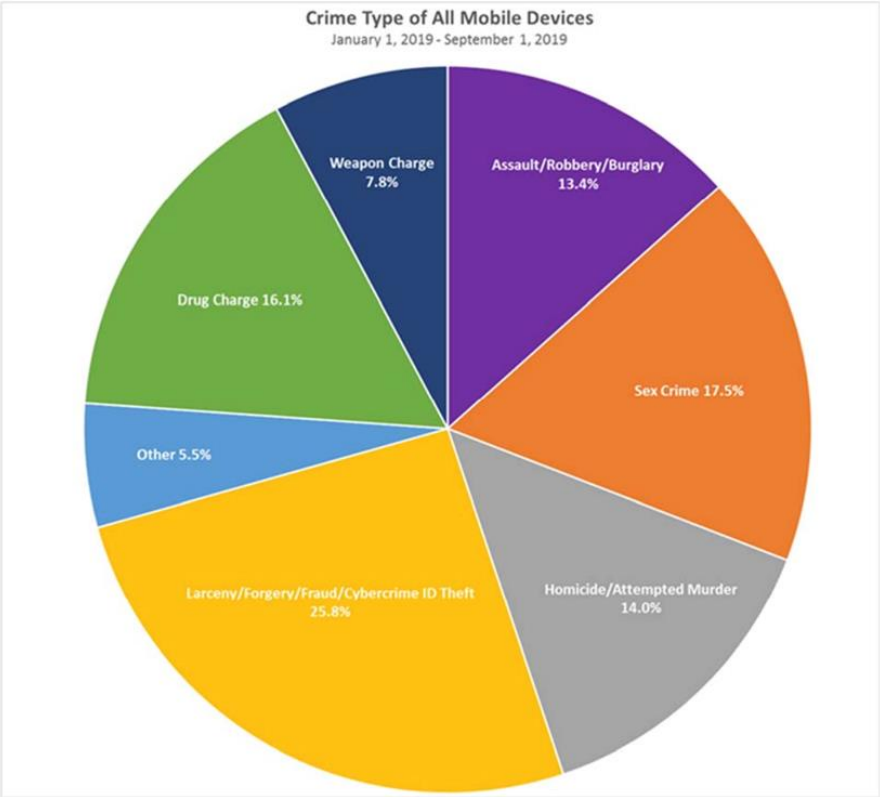
II. A GROWING PROBLEM WITH RAMIFICATIONS FOR OUR PUBLIC SAFETY AND ENTIRE SYSTEM OF JUSTICE

Our most recent internal data from our fifth annual report on Smartphone Encryption and Public Safety[9] puts this growing problem into sharp relief:



First, my Office receives, in criminal investigations, on average 1,600 mobile devices each year, with almost half of those being Apple devices. The percentage of locked Apple devices has increased substantially over the past five years, from 60 percent in 2014 to more than 82 percent in 2019. So that means, for Apple devices alone, we receive over 600 locked and encrypted devices each year.

[9] See *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2018 Report.* https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf



Second, more than 50 percent of the mobile devices that we received in 2019 were connected to investigations into crimes of violence, such as homicides, sex crimes, and assaults.

Our statistics illustrate the alarming frequency in which smartphone encryption forces my Office to investigate and prosecute our city's most serious criminal offenses without access to key evidence. To be clear, we are in some cases able to gain entry into these phones by using lawful hacking tools we've paid hundreds of thousands of dollars to private companies to obtain.

In one notable case, a forensic search of an armed robbery and kidnapping suspect's phone made us aware of numerous text messages that had been exchanged between various unknown parties at or near the time of the kidnapping. These messages had been deleted and were not viewable by investigators – that is until, after months of attempts, a third-party vendor helped us access deleted texts that had been exchanged before, during, and after the kidnapping. This new evidence helped us identify and charge three other culprits.

Such third-party workarounds are cost prohibitive, however, for all but a handful of local law enforcement agencies, like mine in Manhattan. They are simply out of reach for many of **our nation's** smaller and rural communities. And the price we pay doesn't guarantee access, since the process doesn't work in roughly half the cases. The paid workarounds simply give us a better chance of getting into a phone using automated guesses, and Apple and Google have methods to slow

down our rate of guessing. This cat-and-mouse game[10] can stretch across weeks, months, or even years, and that time line is unacceptable for a criminal justice system that has strict statutes of limitations and speedy trial requirements.

This issue also matters in another important way that few people appreciate: in a number of important cases, our ability to open and access phones has led to the exoneration of people wrongly suspected or arrested for crimes.

In one such case, two defendants were identified by eyewitnesses as part of a gang assault in which a large group of people attacked three men and two women. Based on evidence successfully extracted from an encrypted phone, it was determined that the defendants were not present for the assault at all, and they were exonerated prior to trial.

I believe everyone on this commission and Americans generally want to avoid miscarriages of justice. So do I. Our ability to access devices enables us to protect our two-fold obligations – to hold the guilty responsible and to protect the innocent from injustice.

III. SMARTPHONE ENCRYPTION IS A LOCAL LAW ENFORCEMENT PROBLEM

The smartphone encryption debate is often framed as a national security issue. The F.B.I. reportedly paid $900,000 to have a private vendor unlock the San Bernardino shooter's iPhone after Apple told authorities it could not access the device.[11] The mass shooters at Sutherland Springs, Texas[12] and Dayton, Ohio[13] also left behind locked phones that stymied the completion of investigations – investigations that might help communities and law enforcement stop the next mass shooter.

While these are obviously important national cases that demand significant attention and resources, I believe the smartphone encryption debate should center more around the threat it poses to local security in towns across our nation. The majority of collateral damage incurred due to locked mobile devices occurs at the local and state levels, where it is estimated up to 95 percent of American criminal cases are handled. Prosecutors in your home states are all now facing these intractable challenges.

The impact is felt across the country. For instance, it is my understanding that the Florida Department of Law Enforcement alone possessed 418 locked devices as of October 2019. In addition, the Raleigh (N.C.) Police Department had 281, the Tennessee Bureau of Investigation had more than 100, and the Charleston County (S.C.) Sheriff's Office had 70.

---

[10] Ramey, Corinne. "Manhattan DA: Locked Phones Continue to Thwart Criminal Probes." *The Wall Street Journal.* 31 October 18. https://www.wsj.com/articles/manhattan-da-locked-phones-continue-to-thwart-criminal-probes-1541023682

[11] CNBC. "Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer's iPhone. 5 May 2017. https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html

[12] Reigstad, Leif. "Investigators Want Apple to Turn Over Data from the Sutherland Springs Shooter's iPhone." *Texas Monthly,* 20 November 2017. https://www.texasmonthly.com/the-daily-post/apple-iphone-shooting-sutherland-springs/

[13] Wong, Scott and Harper Neidig. "FBI tells lawmakers it can't access Dayton gunman's phone." *The Hill*, 8 August 2019. https://thehill.com/homenews/administration/456742-fbi-tells-lawmakers-it-cant-access-phone-of-dayton-gunman

As I noted earlier, the workarounds by third-party vendors that sometimes succeed for our office are not an option for most local prosecutor's offices, due to the prohibitive costs involved. Thus, two versions of justice exist: one for major cities that can afford such workarounds, and a second for smaller agencies that lack the financial means.

Why should justice be made unattainable for victims in these localities for the sake of Apple and Google's bottom line?

Their decisions to advertise privacy, above all else, make a loud statement that they're not concerned about victims where key evidence is inaccessible due to their locked devices. Earlier this year, no less an authority than Rene Mayrhofer, Google's Director of Android Platform Security, belittled the locking out of law enforcement as an "unintended side effect" [14] of its latest security features.

Unintended or not, the reality remains that these tech titans are doing tremendous damage to our justice system, particularly justice at the local and state levels, by choosing to render themselves incapable of complying with a judge's signed order.

IV. WHY THE CLOUD IS NOT A SUBSTITUTE FOR LAWFUL ACCESS

Law Enforcement is often told that we do not need access to a mobile device to conduct a thorough investigation. Proponents of smartphone encryption say we are living in a "golden age of surveillance," and we should therefore obtain evidence from alternative sources, such as data saved on "the cloud."

My Office does, in fact, regularly obtain evidence from cloud providers pursuant to search warrants, in the form of emails, photographs or videos, and other data that has been backed up from a device.

However, the cloud is an imperfect and incomplete solution to the encryption problem, since the most critical evidence is often only available on a device itself.

This is true for three main reasons:

1. More storage exists on devices than on the cloud. For instance, an iPhone 11 and iPhone 11 Pro come equipped with a minimum of 64 Gigabytes of storage (and, in the case of the iPhone 11 Pro, a maximum of 512 Gigabytes). Meanwhile, Apple provides only 5 Gigabytes of free storage on iCloud by default.[15] Therefore, not all information can be backed up to the iCloud unless a user purchases additional storage data.

2. Even if a user chooses to purchase more data storage, the user has the option to choose which applications to backup to the iCloud. A user can simply decide to not backup

[14] Franceschi-Bicchierai, Lorenzo. "Head of Android Security Says Locking Out Law Enforcement Is an 'Unintended Side Effect.'" *Vice*, 30 January 2019. https://www.vice.com/en_us/article/yw8vm7/android-security-locking-out-law-enforcement-unintended-side-effect

[15] https://support.apple.com/en-us/HT201238

communications, videos, or photos that are incriminating or otherwise critical to an investigation. The user can also opt out of backing up data to the iCloud entirely.

3. Data is available through the cloud only when it has been saved to the cloud. Often a device that is in use during the commission of a street crime – such as a robbery or shooting – is recovered before the evidence is saved by the device to the cloud. The only way to access that data is through the device itself.

V. CHANGING WINDS, DISPELLING MYTHS

Ideally, Apple and Google would do their part to help create a balanced technical and legal solution to the problems caused by their encryption decisions. Absent this contribution, the changing winds of public sentiment around Big Tech, in the wake of Facebook's Cambridge Analytica[16] and Google's Project Dragonfly[17] scandals, has recently created a climate that will support a legislative solution.

Project Dragonfly, in particular, raised a host of questions about Google's planned adherence to China's strict internet censorship rules. Among those questions: if Google is willing to obey an authoritarian government's censorship rules for search engines why won't it do what is necessary to comply with lawful court-ordered search warrants in the United States?

Similar questions on censorship surround Apple's activities in China. Knowledgeable observers suggest Apple – a self-proclaimed champion of consumer privacy in America – does not abide by the same standard when it comes to protecting the privacy of protestors in Hong Kong, because it's better for its bottom line to acquiesce to China's wishes.[18]

To be clear, I, as well as prosecutors across America, are not asking Apple or Google for something extraordinary. We are not asking for a "backdoor" mechanism that would allow our offices to surreptitiously snoop on private citizens. Nor do we want "surveillance" of smartphone communications.[19] Instead, we are asking these companies to comply with warrants issued by impartial judges upon findings of probable cause.

Some in the tech sector have sought to stoke fear that this type of lawful access will morph into a sweeping data collection apparatus that places consumer privacy at risk. I can assure anyone with such a concern that the search warrant process is subject to strict constitutional protections, which have been successfully overseen by impartial courts for over 200 years.

---

[16] Granville, Kevin. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *The New York Times*, 19 March 2018. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[17] Solon, Olivia. "Google's 'Project Dragonfly' censored search engine triggers protests." *NBC News*, 18 January 2019. https://www.nbcnews.com/tech/tech-news/google-s-project-dragonfly-censored-search-engine-triggers-protests-n960121

[18] Matsakis, Louise. "Apple's Good Intentions Often Stop at China's Borders." *Wired,* 17 October 2019. https://www.wired.com/story/apple-china-censorship-apps-flag/

[19] Vance Jr., Cyrus R. "5 ways tech companies distort the encryption debate." *The Washington Post*, 15 December 2015. https://www.washingtonpost.com/news/in-theory/wp/2015/12/15/5-things-tech-companies-dont-understand-about-encryption/

The same cannot be said for Facebook or Google – which harvest our private data, sell it to others for extraordinary profit, and, on occasion, lose millions of people's private information due to hacks. Just last month, we learned that Google's "Project Nightingale" gathers the personal health data of millions of Americans, without informing patients.[20] Likewise, the 2018 security breach that exposed the accounts of 50 million Facebook users[21] demonstrates how the tech companies' priorities are not about protecting privacy after all.

Finally, Facebook CEO Mark Zuckerberg announced in March 2019 planned privacy changes involving end-to-end encryption for Facebook Messenger, WhatsApp, and Instagram.[22] In doing so, Zuckerberg conceded that, with billions of people using these services, there would be some who would use these newly encrypted services for "truly terrible things like child exploitation, terrorism, and extortion." Law enforcement leaders from the U.S., the United Kingdom, and Australia have since signed an open letter publicly opposing these changes.[23]

In 2018 alone, Facebook was responsible for 16.8 million reports of child sexual exploitation and abuse to the U.S. National Center for Missing and Exploited Children.[24] The National Crime Agency estimates these reports resulted in more than 2,500 arrests, with 3,000 children brought to safety. Yet Zuckerberg's announced changes would dramatically restrict the ability to generate these reports: again, because a private company has made a business decision to render its products inaccessible to itself or law enforcement. Simply put, Facebook's planned end-to-end encryption will make it harder to detect – and stop – child abuse and similar crimes.[25]

It's deeply troubling to think the overwhelming majority of these reports would cease if child sex predators were able to "go dark" because of Facebook's business decision. My Office, which is one of the leading anti-trafficking agencies in America, frequently relies on Facebook messages obtained through appropriate judicial process to build cases against traffickers. A world in which children can be recruited and groomed on Facebook – with no hope of law enforcement intervention – is a world in which we, collectively, are failing our children.

---

[20] Copeland, Rob. "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans." *The Wall Street Journal*, 11 November 2019. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

[21] Isaac, Mike and Sheera Frenkel. "Facebook Security Breach Exposes Accounts of 50 Million Users." *The New York Times*, 28 September 2018. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[22] Mark Zuckerberg. "A Privacy-Focused Vision for Social Networking." 6 March 2019. https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

[23] The United States Department of Justice. "Open Letter: Facebook's 'Privacy First' Proposals." 4 October 2019. https://www.justice.gov/opa/press-release/file/1207081/download

[24] Keller, Michael H. and Gabriel J.X. Dance. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" The New York Times, 25 October 2019. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

[25] Farid, Hany. "Facebook's Encryption Makes it Harder to Detect Child Abuse." *Wired*, 25 October 2019. https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/

VI. CONGRESSIONAL ACTION IS REQUIRED TO SOLVE THIS COMPANY-MADE PROBLEM

Five years since the smartphone encryption sea change, it is unconscionable that smartphone manufacturers, rather than working with government to address public safety concerns, have dug in their heels and mounted a campaign to convince their customers that government is wrong and that privacy is at risk. Because Apple and Google refuse to reconsider their approach, I believe the only answer is federal legislation ensuring lawful access. Tech goliaths have shown time and again they have no business policing themselves.

Of course, as in any industry – especially when it comes to public safety – federal regulation has been important for many decades in the communications industry.

For example, when telephone companies went from using copper wires to using fiber optics and digital signals, law enforcement could no longer rely on previous technology when it came to wiretaps, so Congress passed the Communications Assistance for Law Enforcement Act (CALEA), mandating that telecom providers build into their systems mechanisms for law enforcement to install new forms of wiretaps when approved by a court. CALEA has worked. It has saved lives, and it has withstood constitutional challenge. It has not stifled innovation, as its opponents feared. And it has not caused American consumers to migrate to foreign competitors in search of greater privacy.

The same is true in the financial services industry. Beginning in the 1970s, as law enforcement learned more about how criminals were using banks to move money, Congress passed new laws to require financial institutions to adopt new technologies and procedures to detect money laundering; to better know their customers; to maintain customer data; and to make that data available to law enforcement pursuant to a court order. Over time, government and industry came together to develop protocols and procedures to effectively implement those new laws, and a broad consensus emerged. Banks and investment firms did not want to be conduits for crime and terror.

My sincere hope is that, with appropriate congressional leadership and legislation, a similar result can be achieved with this industry, too.

If Apple were participating in today's panel, its representative would likely tell you it is impossible to maintain keys to open one of their devices without creating a hole for cryptocriminals themselves to gain access. I have two responses to this:

- First, in 2016, Apple's then-general counsel acknowledged that the company's process for unlocking phones in response to warrants prior to 2014 had never led to a security breach. [26]

- Second, this new criminal justice problem is the direct result of these private companies' decisions to redesign their products. I'm not a technologist, but I'm confident the problem can be solved by a company re-design as well. As President Kennedy once said,

[26] Bruce Sewell, Senior Vice President and General Counsel for Apple, Inc., Responses to Questions for the Record, "The Encryption Tightrope: Balancing Americans' Security and Privacy," at p. 2. Question 6(b)(1). U.S. House Committee on the Judiciary, 1 March 2016.

> "Our problems are man-made, therefore, they can be solved by man. No problem of human destiny is beyond human beings."

To that end, I would offer three recommendations to this Commission:

First, that federal legislation is necessary for law enforcement to break the encryption stalemate that prevents us from obtaining evidence subject to a court-ordered search warrant from smartphone and social media giants. Since they've made a business decision valuing privacy above public safety, I believe it's imperative that Congress acts to protect our citizens.

Second, the Commission should urge tech companies and law enforcement to meet on a regular basis to discuss lawful access and finding paths forward.

Third, while the entire lawful access ecosystem including "data in motion" must be addressed, restoring lawful access to "data at rest" on smartphone devices is an immediately achievable solution that would help state and local law enforcement confront the challenges we face. This "data at rest" middle ground on encryption is the position "most likely to enable fruitful debate among diverse communities-of-interest," according to the Carnegie Endowment for International Peace. [27]

Thank you for inviting me to testify and for your continuing efforts on this issue.

[27] Carnegie Endowment for International Peace, "Moving the Encryption Policy Conversation Forward," September 2019. https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

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.

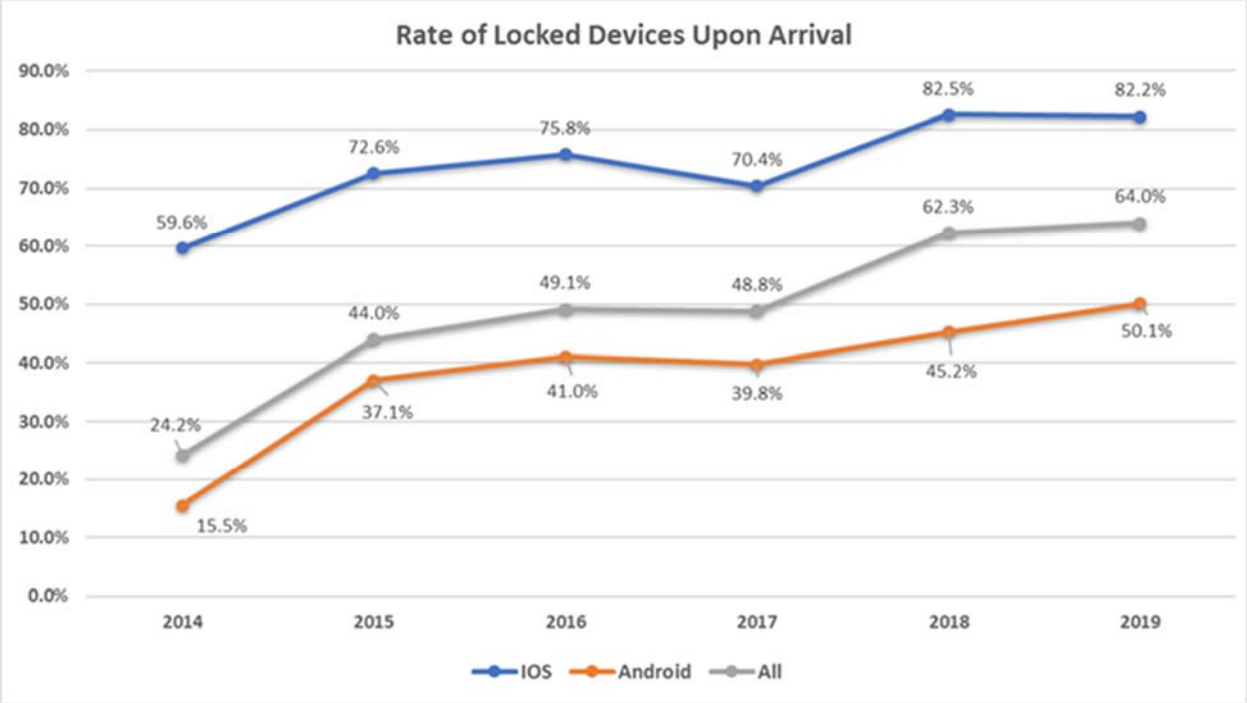
[7] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2017 Report*, Nov. 2018, *available at* https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf.

[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]

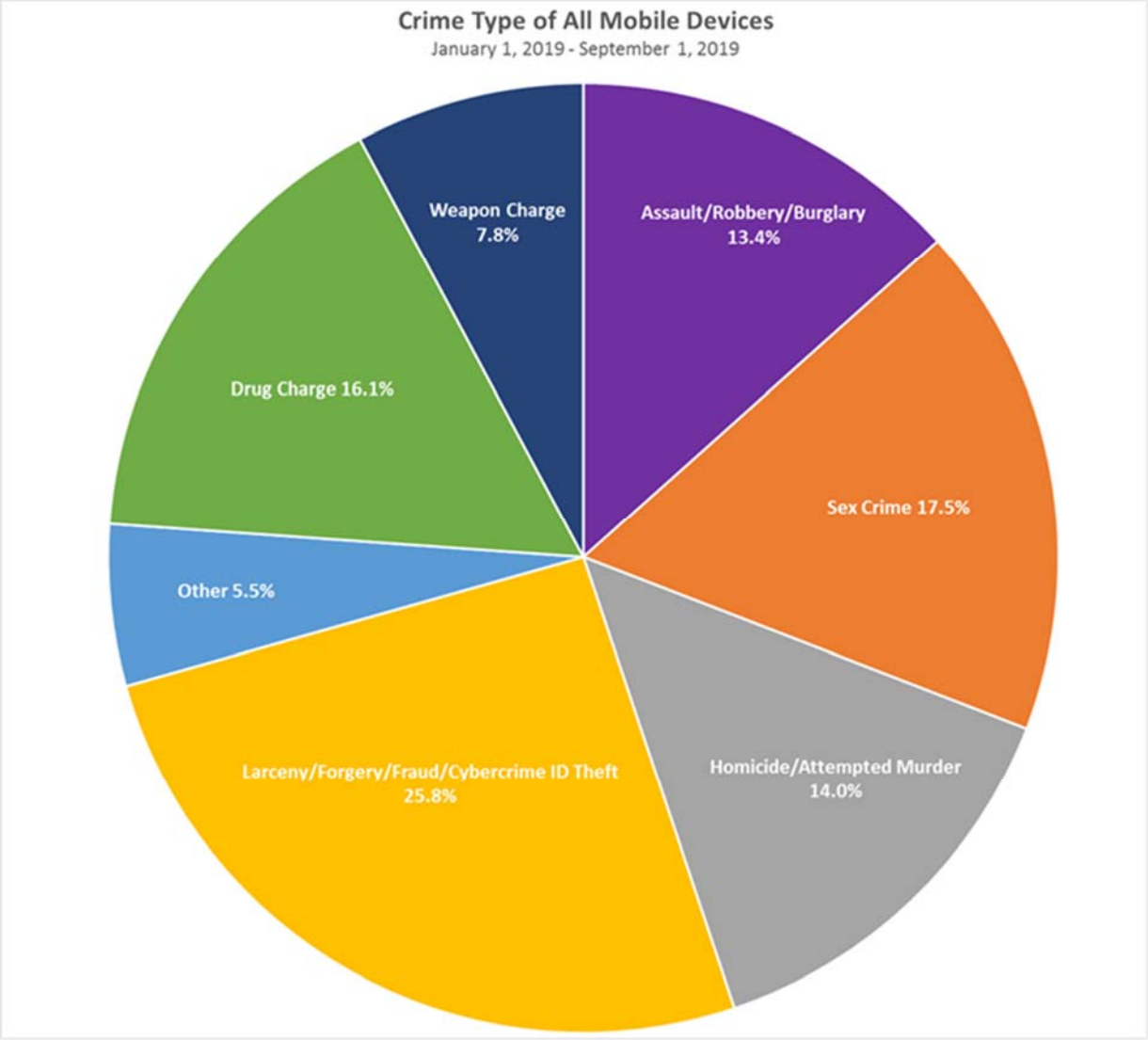
For our office and others, the number of encrypted devices containing important evidence remains high, with the trend of inaccessibility increasing each year. As the below chart indicates, the percentage of encrypted Apple devices arriving at our office has increased significantly over the past five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

Darrin Jones

Assistant Director, Federal Bureau Investigations

Darrin E. Jones was appointed as the Executive Assistant Director of the FBI's Science & Technology Branch in April 2020. In this capacity, he supervises the executives and operations of the FBI Laboratory Division (LD), the Criminal Justice Information Services Division (CJIS), and the Operational Technology Division (OTD).

Mr. Jones began his FBI Career in September 1997 as a special agent in the Salt Lake City Division where he investigated international drug trafficking, cybercrime, and he helped lead the counterterrorism planning for the 2002 Olympics. In 2003, Mr. Jones was promoted to supervisor in the Office of Congressional Affairs at FBI Headquarters, where he served as a liaision for the FBI on technical issues with members of Congress and their staff.

In 2005, Mr. Jones was assigned as a supervisor to the FBI's Operational Technology Division (OTD) at Quantico, Virginia. In this role, he was responsible for the creation of the FBI's Technical Liaison Office and the cultivation of close working relationships between the FBI and high technology companies both domestic and foreign.

In 2007, Mr. Jones was assigned to the Albuquerque Division as the supervisor overseeing the division's cyber program. In this role, Mr. Jones managed criminal cyber cases as well as national security intrusion investigations. In 2009, while assigned to the Albuquerque Division, Mr. Jones was responsible for coordinating the building of the FBI-led New Mexico Regional Computer Forensic Laboratory (NMRCFL), providing state-of-the-art digital forensics services to the law enforcement and national security communities. Following its completion, Mr. Jones served as the Director of the NMRCFL.

In 2011, Mr. Jones was appointed assistant special agent in charge of the Anchorage Field Office. Two years later, Mr. Jones returned to Washington, D.C., where he was named section chief of the Communications Intercept Section, OTD. Mr. Jones oversaw technical and policy matters associated with both criminal and national security-related electronic communications interception.

Mr. Jones was appointed as Special Agent in Charge (SAC) of the Kansas City Division in March 2017. In this position, Mr. Jones oversaw the Kansas City Division headquarters and eight satellite offices that together covered the entire state of Kansas and the western district of Missouri. As SAC, Mr. Jones developed close relationships between the FBI and regional law enforcement partners, including joint management of the Heart of America RCFL (HARCFL), and establishing a robust violent crimes task force in cooperation with the Kansas City Police Department and other federal, state, and local partners.

In June of 2019, Mr. Jones was appointed as an Assistant Director in the IT Infrastructures Division then transitioned to the role of Assistant Director in Deputy Director's Office for the FBI's Lawful Access initiative.

Mr. Jones earned a Bachelor of Science degree from the University of Nebraska. In 2018, Mr. Jones earned an advanced certification in Information Security from Carnegie-Mellon University. A native of Nebraska, Mr. Jones is married and the father of two children.

Charles L. Cohen

Vice President, NW3C

Chuck Cohen is Vice President at NW3C, The National White Collar Crime Center. He is a Professor of Practice in the Indiana University Bloomington Department of Criminal Justice, where he has taught since 2003. Chuck serves as an Auxiliary Detective with the Indiana University Police Department, providing technical assistance and giving him statewide police authority.

Chuck is a retired Indiana State Police Captain, where he served for over 25 years. He was most recently the Commander, Intelligence and Investigative Technologies. In this capacity, Capt. Cohen was responsible for the cybercrime, electronic surveillance, technical services, and Internet crimes against children units along with overseeing the department's overt and covert criminal intelligence functions. Chuck was the Indiana Intelligence Fusion Center Executive Director and Indiana Internet Crimes Against Children (ICAC) Task Force Commander.

Chuck's formal education includes a Master of Business Administration from Indiana Wesleyan University and an undergraduate degree from Indiana University with a double major in Criminal Justice and Psychology. Chuck is also a Certified Fraud Examiner and Certified Economic Crime Forensic Examiner.

He speaks internationally on topics including the implications of online social networks in criminal investigations and criminal intelligence gathering, cybercrime, online fraud, money laundering, corruption investigations, and the investigation of skilled criminal offenders. He has trained investigators and analysts on five continents.

Chuck testified to the 114th Congress in 2016 as a subject matter expert on encryption. He was a member of the Office of the Director of National Intelligence Summer Hard Problem Program in 2008, 2009, and 2010. He sits on the IACP Cyber Crime & Digital Evidence Committee and serves as an Association of State Criminal Investigative Agencies Cyber Crime Committee Subject Matter Expert. Chuck is a charter member of the International Association of Cyber & Economic Crime Professionals.

He is a published author, including peer-reviewed material and a cover article for *Police Chief Magazine*. Chuck was featured on the cover of the National White Collar Crime Center's *Informant* magazine and a featured guest on the syndicated radio program, "The Badge" on SiriusXM. He was a subject matter expert for a Fox nationally syndicated show regarding criminal activity in online dating sites and for the Canadian Broadcasting Corporation's national news regarding criminal activity in Virtual Worlds.

Recent and Noteworthy Presentations:

2011 – 2016 & 2019	**International Communications and Digital Forensics Conference**—London, UK Co-Sponsored by Home Office and Metropolitan Police Service Digital Communications Group
2018	**International Association of Chiefs of Police**—Delhi, India *"Policing Challenges in 2020, How is Cyber Space Shaping Our Approach to Cybercrime & Terrorism; How do we Perform Within it and Take Advantage of it?"*
2018 & 2015	**Calgary Cyber Summit—**Calgary, CA Keynote Speaker to an audience of over 300 attendees
2017	**Police Scotland**—Tulliallan, UK Multiple day training at Scottish Police College
2010 – 2020	**ISS World Conferences**—Washington, D. C.; Dubai, UAE; Kuala Lumpur, MY; Johannesburg, SA; Brasilia, BR; Mexico City, MX; Panama City, PA; and Prague, CZ
2016	**International Association of Crime Analysts Annual Conference**—Louisville, KY Keynote plenary speaker
2014 & 2015	**National Cyber Crime Conference**—Boston, MA Keynote speaker to an audience of over 600 conference attendees
2010	**MAGLOCLEN Annual Conference**—Columbus, OH Keynote presenter
2009	**E-Crime Congress**—London, UK *"Real Crimes in Virtual Worlds."* Routinely trained members of the Intelligence Community along with federal, state, local, and private entities

Written Testimony

Charles L. Cohen, Vice President
NW3C, The National White Collar Crime Center

Technology Used to Perpetrate Crime
The Dark Web, Child Exploitation, and Human Trafficking

April 15, 2020

Background:

The Oxford English Dictionary defines the Dark Web as *the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.* The same dictionary uses the sentence example *the Dark Web poses new and formidable challenges for law enforcement agencies around the world.*[i] There could be no more accurate use of the phrase Dark Web.

The World Wide Web became available in about December 1990 and is designed in such a way that domains are registered worldwide by a nongovernmental organization called the Internet Corporation for Assigned Names and Numbers (ICANN), while a division a division of ICANN called the Internet Assigned Numbers Authority (IANA) organizes the hosting and addressing of those sites. The Surface Web (also called the Visible Web, Indexed Web, or Indexable Web) refers to portions of the World Wide Web that are searchable by using common search engines such as Google, Bing, and Yandex. The Deep Web refers to portions that are not searchable by using these search engines, but can still be accessed from a browser (e.g. Firefox, Chrome, and Safari) if the domain name and file path are known. It is relatively easy to determine in both instances, either through publicly available information or through the service of legal process, who has registered a particular domain and where it is hosted.

The Dark Web is differentiated from both the Surface Web and Deep Web in several ways that pose significant challenges to law enforcement. The Dark Web is not a single thing, but rather several networks which use complex techniques that can conceal and obfuscate a user's identity as well as the location of those accessing Surface websites, making it nearly impossible for law enforcement to trace criminal activity.

Common Dark Web networks include Tor, I2P, Freenet, anoNet, RetroShare, DHT, GNUnet, Zeronet, OneSwarm, Mixminion, AntsP2P, Tribler, and several others. All of these networks are free and easily accessible in the United States and countries like the United States. All of these use forms of onion routing, layer routing, overlay networks, or other techniques to facilitate the obfuscation. In the case of Tor, this is accomplished through the use of over 7,000 relay and bridge servers around the world through which traffic is routed[ii]. About 2 million people use Tor every day.[iii]

Several Dark Web networks also allow for the creation of domains that are not registered by ICANN and thwart the ability to determine server control and location. In April 2020, there were between 90,000 and

100,000 such Tor Hidden Service servers.[iv] Those servers ranged from ones maintained by global companies to ones placed by individuals in a spare bedroom. Due to the nature of the technology, it is often not possible for law enforcement to determine a Tor Hidden Service server's location. Those who maintain such servers for criminal purposes often employ additional technological and social safeguards against law enforcement investigation and interdiction.

It can be helpful to think of a ship when conceptualizing the differences among Surface Web, Deep Web, and Dark Web servers. The Surface Web is made up of the publicly and easily accessible decks and passageways leading to registered cabins with names and numbers on each hatch. For the Surface Web, this is accomplished by ICANN and search engines. The Deep Web is analogous to unmarked compartments and hatches that are sometimes publicly accessible if someone tells you where to look and sometimes are only accessible with special permission from a steward. The Dark Web can be represented by unknown and intentionally hidden passageways, cabins, and compartments that are not mapped, visible, or in the ship's blueprints. These areas of the ship require specialized understanding and special keys to identify and access the cabins and their compartments.

Child Exploitation on the Dark Web:

Peer-reviewed published research by University of Massachusetts Amherst Professor Brian Levine and his colleagues in 2017 found that 65% of all content on the Dark Web tool Freenet was Child Sexual Abuse Material (CSAM),[v] which is also known as child pornography. The FBI reports that one Tor Hidden Services server, known as Playpen, had more than 150,000 users who actively traded in CSAM. A lengthy and highly complex investigation revealed that the creator of Playpen lived in Florida while two administrators lived in Indiana and Kentucky. The interdiction of the Playpen server led to a transnational investigation, which resulted in the rescue over 350 children and the arrest of over 850 offenders.[vi]

While Playpen no longer exists, and the people responsible for its creation and maintenance are serving lengthy terms of imprisonment, several other Tor Hidden Service servers have succeeded it to provide a covert method of dissemination and receipt of CSAM. I have personal knowledge as a criminal investigator of one such server that is currently active and continually has at least 800 concurrent connections. However, due to the nature of Tor and Tor Hidden Service Servers, it is not possible to determine the identity of those who created or maintain the server(s), the location of the server(s), or those who are using this platform to disseminate and receive CSAM.

One investigation conducted in Indiana demonstrates the challenges that law enforcement routinely faces when offenders use free, easy-to-use, and easily available Dark Web networks. Buster Hernandez pled guilty in the Southern District of Indiana on February 6, 2020, to 41 counts, including: eight counts of Production of Child Pornography, three counts of Coercion and Enticement of a Minor, four counts of Threat to Use an Explosive Device, and ten counts of Threats to Kill, Kidnap, and Injure.[vii] Mr. Hernandez told one child victim that he wanted to be, "the worst cyberterrorist that ever lived." At the time of his arrest in August 2017, Mr. Hernandez was 26 years old, unemployed, living in California, and had no specific education or training in internet technology. Following his arrest, United States Attorney for the Southern District of Indiana Josh Minkler said in a press conference that it took over 19 months of the combined investigative efforts of the

Indiana State Police and FBI to collect evidence sufficient to identify and locate Mr. Hernandez. USA Minkler said that those investigative efforts included over 100 state and federal search warrants; more than 200 grand jury subpoenas; court authorization for over 20 types of electronic surveillance, including a Title III electronic wiretap; "hundreds of hours of surveillance;" and "a device called a NIT [Network Investigative Technique]".[viii] Mr. Hernandez's primary criminal tradecraft was the use of Tor, which comes pre-installed with a free and easy-to-use operating system that is designed to run in volitile memory and leave no traces on a computer system when it is turned off. He used this operating system and Tor to access Surface Web social media and cloud storage sites that he then used to facilitate his crimes.

In addition to hindering individual investigations, Dark Web networks also drain already overburdened law enforcement resources related to the investigation of child exploitation and trafficking. During the 19 months while the investigation of Buster Hernandez was ongoing, the Indiana Internet Crimes Against Children Task Force received over 5,000 CyberTips from the National Center for Missing and Exploited Children (NCMEC) related to child pornography, online child solicitation, and online child sexual extortion.

Law Enforcement throughout the United States and world faces similar challenges. Houston Police Chief Art Acevedo describes Houston as "ground zero" for human trafficking. He further states that the Houston Area Internet Crimes Against Children Task Force found that in the 30 days prior to September 19, 2019, 64.6% of the over 2,300 cases under investigation involved the use of services that mask offender identity. The increasing use of the Dark Web by offenders exacerbates existing challenges associated with the overwhelming number child exploitation and sex trafficking cases requiring investigation.

Trends in the Dark Web:

While the World Wide Web has existed since 1990 and Tor has existed since 1996, the Surface Web and Dark Web have existed as two distinct things. Over the last few years, there has been a shift from that which can be considered Surface Web or Deep Web to that which can best be described as Dark Web. As the result of several factors, there is an increasing acceleration of this transition. These factors should not be viewed independently, but rather as an interrelated set of factors that are choking off the ability for criminal investigators to identify and locate both offenders and victims and preventing access to evidence. As a practitioner, what I see is a rapid evolution toward what was once the Surface Web becoming just one more area of the Dark Web.

One factor that is causing the shift to Dark Web is the increased availability and sophistication of anonymous proxies and virtual private networks (VPNs). Numerous companies advertise VPN services that accept payment with a variety of cryptocurrencies, are located in countries that do not have Mutual Legal Assistance Treaties (MLATs) with the United States, and do not maintain any log files. This is combined with a relatively recent trend toward use of VPNs by criminals, including during the trading of CSAM on Peer-to-Peer networks. The ability to share files peer-to-peer via the Internet has existed since Napster was released in 1999. Offenders have used these networks since that time to disseminate CSAM images and videos. Law enforcement has also had effective tools for many years with which it could conduct investigations related to these crimes. But, there has been a recent and rapid increase in the use of bulletproof VPNs, Tor, and other Dark Web

capabilities in the distribution of CSAM files. Such tools cripple the ability of law enforcement to conduct investigations involving the distribution of contraband CSAM via peer-to-peer networks.

One Law Enforcement Sensitive tool can identify over four million image and video files that contain chargeable CSAM. The administrator of this tool approved me to include in my testimony today that during federal fiscal year 2019, 24.97% of all peer-to-peer sharing of contraband CSAM files was obfuscated by the use of VPNs and Tor. The use of these counter-investigative capabilities is rapidly increasing. The same law enforcement tool found only 5% of contraband CSAM file sharing to be hidden in this manner 18 months prior. Peer-reviewed published research conducted in 2013 found only .045% of sampled peer-to-peer file sharing to be hidden in this manner.[ix]

As an example of the depth of this problem, between January 16 and April 10 of this year, one IP address associated with a VPN provider located in the United States that does not maintain logs as a matter of policy was seen by the law enforcement tool to be disseminating CSAM files more than 160,000 times. That single IP address was associated during these 55 days with the distribution of 413,959 previously identified CSAM files, including 38,925 images or videos depicting that which meets federal sentencing enhancement standards for sadistic or masochistic abuse of children.

Another factor that is causing the shift to Dark Web is the increasing prevalence of end-to-end encryption by large Internet Service Providers. People send more than 21 billion photos through Facebook Messenger every month. Messenger accounts for more than 10% of all mobile VoIP calls globally.[x] NCMEC estimates that in 2018, Facebook submitted nearly 12 million CyberTips related child exploitation and child sex trafficking specifically associated with Messenger.[xi] While Apple does not publish information about the amount of communication via iMessage, as of 2017 there were 728 million iPhones in use worldwide.[xii] NCMEC is quoted in the New York Times as reporting that Apple submitted a total of only 43 CyberTips in 2018,[xiii] and Apple reported only 205 CyberTips last year.[xiv] Apple iMessage and Facebook Messenger are substantially similar in function. One notable difference is that iMessage communication is end-to-end encrypted while communication via Messenger is not currently encrypted. In the first quarter of 2019, Facebook began publicly expressing an interest in encrypting Messenger and other communications, to which the United States Department of Justice and several other countries have expressed strong objections.[xv],[xvi],[xvii]

A third factor that is causing the shift to Dark Web is the inability in many instances for law enforcement to be able to identify the person or business that might hold evidence or information related to child exploitation or human trafficking. When there is a need to obtain evidence from, or make an emergency request for information in a life-or-death emergency to, a Surface Web or Deep Web registrant or site host it is generally possible to obtain contact information. This provides an entity to which law enforcement can make an exigent circumstance request or on which legal process can be served. This contact information most commonly includes a name, address, telephone number, email address, host address space, and other information. Even when that company is located outside the United States, there are existing mechanisms, such as the MLAT process, to obtain information that might aid in the rescue of a child or be of evidentiary value. These mechanisms will hopefully be improved with the advent of the CLOUD Act.

The shift from browser-based online communication to app-based online communication is rapidly removing the ability of law enforcement to obtain contact information when needed in the course of a criminal investigation. There are currently about 1.8 million iOS apps available in the Apple App Store.[xviii] There are over

2.8 million Android OS apps available in the Google Play Store.[xix] Offenders routinely use communication, image hosting, video sharing, file hosting, gaming, dating, and social media apps to exploit and traffic in children. With the exception of those apps that are associated with large companies that have companion Surface Web sites, it is often not possible for law enforcement to identify or locate the person, people, or business that created the app or might retain information associated with the use of that app.

Before making recommendations, it is important to note that the examples in my testimony focused on child exploitation and human trafficking because that is the topic on which the commission asked me to provide information. The commission should be aware however that despite the prevalence and continued growth of CSAM on the internet, Americans are subject to: increasing financially-motivated cyber crime that threatens our economy; intellectual property theft that threatens our National sovereignty; espionage and terrorist acts that threaten all of our personal safety and National security; the illegal sale of narcotics including opiates that right now are killing our children; illegal weapons transactions that facilitate violent crime and gang warfare; and many more organized criminal activities, at the hands of criminal enterprises that thrive in light of the technologies we discuss today and the increasing limitations placed on law enforcement to obtain information and evidence through the service of legal process or lawful technical investigative methods.

Recommendations:

1. Fund and make available consistent and high-quality training and technical assistance on a large scale for state, local, territorial, and tribal (SLTT) law enforcement related to all issues outlined in this testimony. With increasing frequency during the normal course of business, SLTT law enforcement inadvertently encounters the sexual exploitation and trafficking of children in which various aspects of Dark Web technologies are being used. Also, SLTT law enforcement now routinely encounters Dark Web technologies in the course of conducting investigations focused on the sexual exploitation and trafficking of children.

2. Implement regulations and laws that require Internet Service Providers and companies providing commercial VPN services to retain certain records and set record retention periods. A model for this is the Bank Secrecy Act of 1970 and subsequent anti-money laundering legislation, which set record retention and retention period requirements for financial institutions.

3. Update the Communications Assistance for Law Enforcement Act (CALEA) of 1994 to require that Internet Service Providers provide assistance to law enforcement similar to that which CALEA currently requires for landline and cellular carriers, which increasingly provide similar services. This includes such assistance for law enforcement when the communication is encrypted. It is noteworthy that both CDMA and GSM cellular protocols are encrypted and widely understood to be secure for users. Nonetheless, cellular carriers are compliant with CALEA in providing investigative assistance to law enforcement.

4. Make a resource that provides current and correct contact information for apps offered in the Apple App Store and Google Play Store readily available to law enforcement. This can be accomplished through a requirement that Apple and Google maintain, and make available to law enforcement, such information for all apps available in the United States version of the App Store and Play Store.

[i] https://www.lexico.com/definition/dark_web, accessed April 12, 2020.
[ii] https://metrics.torproject.org/networksize.html, accessed April 12, 2020
[iii] https://metrics.torproject.org/userstats-relay-country.html, accessed April 12, 2020
[iv] https://metrics.torproject.org/hidserv-dir-onions-seen.html, accessed April 12, 2020
[v] http://ceur-ws.org/Vol-1873/IWPE17_paper_12.pdf, accessed April 12, 2020.
[vi] https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years, accessed April 12, 2020.

[vii] https://www.theindychannel.com/news/local-news/crime/suspect-in-brian-kil-threats-case-pleads-guilty-to-all-federal-charges, accessed April 12, 2020.
[viii] https://www.kgun9.com/news/national/26-yr-old-from-california-charged-in-brian-kil-plainfield-school-threats-case, accessed April 12, 2020.
[ix] Li et al., "An overview of anonymity technology usage", *Computer Communications*, Volume 36, Issue 12, July 1, 2013, pages 1269-1283.
[x] https://www.messenger.com/messengerfacts, accessed April 12, 2020.
[xi] https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html, accessed April 12, 2020.
[xii] https://www.statista.com/statistics/755625/iphones-in-use-in-us-china-and-rest-of-the-world/, accessed April 12, 2020.
[xiii] https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html, accessed April 12, 2020.
[xiv] https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers, accessed April 12, 2020.
[xv] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/, accessed April 12, 2020.
[xvi] https://www.justice.gov/opa/press-release/file/1207081/download, accessed April 12, 2020.
[xvii] https://cdn.vox-cdn.com/uploads/chorus_asset/file/19446144/Facebook_Response_to_Barr_Patel_Dutton_Wolf___1_.pdf, accessed April 12, 2020.
[xviii] https://www.lifewire.com/how-many-apps-in-app-store-2000252, accessed April 12, 2020.
[xix] https://www.appbrain.com/stats/number-of-android-apps, accessed April 12, 2020.

Bryan P. Stirling

Director, South Carolina Department of Corrections

Bryan P. Stirling was confirmed as the Director of the South Carolina Department of Corrections by the South Carolina Senate on February 19, 2014. With a staff of 5,000, Stirling is also responsible for roughly 19,500 inmates currently serving time in one of the 21 penal institutions across the state.

Upon assuming office, Director Stirling oversees an agency that has undergone officer shortages and media scrutiny. Under Stirling's leadership, the agency has closed six institutions. The inmate population has declined due to a reduction in the recidivism rates, sentencing reform, successful programs and services within the institutions. Stirling settled a decade old mental health lawsuit that plagued the agency and its leadership.

Stirling has been recognized for his passion and dedication to improving public safety, as well as, making each institution a safe, secure and productive environment where offenders are given the skills and resources they need for a future that spans far beyond their prison cell.

In 2016, Stirling received the Stephen G. Morris Nelson Mullins Social Justice Award from the Columbia Urban League and the William D. Leeke Award of Excellence.

Prior to joining the correctional system, Director Stirling served as Deputy Attorney General for nearly six years. Most recently, he served Governor Nikki Haley as her Chief of Staff from October 2012 to September, 2013, during which he oversaw management of the governor's cabinet and the Office of Executive Policy and Programs. Stirling graduated from the University of South Carolina in 1991 and USC's School of Law in 1996.

Bryan Stirling – Testimony for April 15, 2020 Panel

Thank you, President Trump for signing an executive order establishing the Presidential Commission on Law Enforcement and the Administration of Justice for the first time in a half century. Also, thank you to the Commission Chairman Keith and the entire Commission for your time on this very important public safety matter.

Contraband cell phones are the most dangerous weapon an inmate can possess and pose a serious threat to public safety and prison safety. Correctional officials have been grappling with this problem for more than a decade. With technology, inmates are only taken out of society for public safety physically however virtually they are out there still committing crimes. Please see the attachment for just a sample of crimes that have been committed by South Carolina inmates via contraband cell phones. The Federal Executive Branch or Congressional Branch can solve this very dangerous public safety issue.

In that vein, we are seeking the following:

1. A Federal Communications Commission interpretation of the Communications Act of 1934 that would permit states to use jamming technology to block the signals from unauthorized cellphones to prevent their use by prison inmates. Specifically, we are seeking an interpretation stating that signals originating from a contraband cell phone inside of a correctional institution are not "authorized," as defined by the Communications Act of 1934. When states enact laws deeming cell phones possessed by inmates "contraband," use of a cell phone in prisons is not "authorized" and illegal. Consequently, states with such laws should be permitted to use jamming technology to block the signals from these unauthorized cell phones to prevent their use by prison inmates.

2. Hearings in the Congressional committees of jurisdiction or before the Commission. This would allow sworn testimony by corrections leaders, as well as the Department of Justice, the Department of Commerce, and the wireless industry about the problem, possible solutions, and the state of jamming technology.

3. Support regarding a statutory change to allow state and local prisons to use jamming devices. There are bills pending in both chambers of Congress that would make the change (S.952/H.R. 1954, The Cell Phone Jamming Reform Act of 2019).

4. Creation of a pilot program that would allow jamming in four states and building in an evaluation component to test the effectiveness and feasibility of jamming technology.

5. Further research and testing to augment Managed Access System technology that would make such systems - which are currently highly complicated and extremely cost-prohibitive - actually work for state and local prisons.

Preventing the influx of contraband in prisons has always been a serious concern of, and a difficult challenge for, correctional institution administrators. In the hands of inmates, cell phones undermine the foundation of the criminal justice system by allowing convicted criminals to further their criminal activities behind bars. Through the use of contraband cell phones, inmates are able to coordinate illegal drug shipments, direct acts of violence, perpetuate gang activity, commit acts of fraud, and plan escapes. Today, the methods by which prisoners and their contacts outside the prison walls can introduce contraband have increased, and these criminals are now incorporating state-of-the-art technology to include the use of drones. South Carolina is one of several states that has already dealt with drones delivering contraband cellphones to prisoners. Prisons are designed to keep people in, not to keep contraband out. Consequently, each year, tens of thousands of contraband cell phones are confiscated within the walls of America's prisons. When someone is convicted of a crime they are physically taken out of society but virtually still able to victimize society because of contraband cell phones.

In the past few years, the South Carolina Department of Corrections has installed thermal imaging cameras and magnetic static detectors and has built surveillance towers at two of our maximum-security facilities. We have asked for assistance from the public and created an online tool for anonymous reporting of the use of cell phones or social media by prisoners. There is a law in place that makes furnishing or attempting to furnish contraband, including cell phones, a felony carrying up to ten years in prison (S.C. Code 24-3-950). Many individuals, including our own corrections staff members, have been arrested for violations of this law.

However, despite these efforts, we continue to lose the war on contraband. Canine detection, scheduled disruptions, frisk searches, pat downs, x-ray machines, metal detectors, boss chairs, vehicle searches, stationary and roving perimeter posts, and magnetic static detectors fail to put even a dent in the massive wave of telecommunications devices that infiltrate our institutions. The effort to stop the onslaught becomes more dangerous for our staff by the day because the money being made is substantial and inmates will stop at nothing to ensure their prison economy thrives.

A cell phone in the hands of an offender is a weapon, just as lethal as a prison-made shank. Look no further than South Carolina's own contraband officer, Captain Robert Johnson, who found himself within inches of his life after he was shot six

times in his own home in retaliation for successfully impeding the flow of contraband at Lee Correctional Institution located in Lee County, South Carolina. The hit on his life was orchestrated from inside the prison walls by an inmate using a contraband cell phone. Unfortunately, the attempt on Captain Johnson's life is only one of many similar incidents across the country. For example, in Tennessee, a veteran correctional officer was assassinated after a plot to murder him was orchestrated via a contraband cell phone. (See https://fox17.com/news/local/tennessee-corrections-commissioner-calls-for-use-of-cellphone-jamming-technology.) In North Carolina, a high-ranking gang leader attempted to direct a contract killing of a prosecutor's father through use of a contraband cell phone (Charlotte Observer, May 31, 2017). In New Jersey, an inmate using a smuggled contraband cell phone ordered the shooting death of a mother of two (Chris Megeria/Statehouse Bureau-Trenton, N.J., June 10, 2010). These are merely examples; similar stories can be found across the country.

As technology continues to advance, so does the risk of that technology being used in a dangerous manner inside a prison. Cell phones are now powerful handheld computers. State prison officials must be able to use the latest and most up-to-date technology to keep their staff, the facilities, the public safe and frankly the offender themselves safe. Prison administrators need to be able to respond to the danger posed by contraband cell phones using methods that can actually neutralize the danger.

As illustrated above, inmate access to contraband cell phones is one of the most serious correctional security and public safety issues facing state prisons across the country. However, an antiquated federal law from 1934, as interpreted by the Federal Communications Commission, currently prevents state and local prisons from using the most effective method to combat the threat: cell phone jamming systems. (See Federal Communications Act of 1934, 47 U.S.C. § 333; see also 47 C.F.R. § 2.803; 18 U.S.C. § 1362 & -1367(a).) Significantly, there are exceptions in this law for "the Government of the United States or any agency thereof;" therefore, federal institutions are allowed to use jamming technologies. (See 47 C.F.R. § 2.807). Like federal prisons, state and local prisons must be allowed to implement cost-effective cell phone jamming technologies to stop this dangerous threat to public safety. Particular solutions may vary from state to state and from facility to facility, and what works for one state may not work for another. Similarly, what may be deemed affordable by one state may not be cost efficient for another. Determinations of this kind are uniquely state functions that should not be impeded by outdated federal laws and regulations.

Managed Access Systems are one tool being used by state corrections officials to attempt to combat the danger posed by contraband cell phones. In fact, South Carolina is currently using a Managed Access System at one of its maximum-security

prisons. However, Managed Access Systems are extremely expensive and require constant monitoring. Furthermore, Managed Access Systems only work when all of the right variables are in place. Managed Access Systems must "impersonate" all commercial cellular carriers who offer service in the area, meaning the system must support every radio frequency and cellular technology used by the carriers to "trick" the contraband cell phones into connecting to the Managed Access System instead of the commercial cellular network. This becomes increasingly challenging as cellular technologies evolve and each successive generation (i.e., 2G, 3G, 4G, 5G) incorporates more sophisticated network authentication and encryption methods. Additionally, a Managed Access System must also have a sufficient signal strength margin over the commercial cellular base stations to ensure that the contraband cell phones connect to the Managed Access System one-hundred percent of the time. In order to avoid "bleed-over" into areas outside the prison walls, a Managed Access System must carefully monitor and control the strength of the radio signal. Problems managing the signal strength increases both the cost of the system and the points of potential failure. While cell phone jamming technology faces similar challenges with respect to radio signal strength, cell phone jamming systems only need to ensure coverage of all radio frequencies in use by the cellular carriers with no concerns for the underlying (and ever-changing) cellular technologies. Accordingly, cell phone jamming systems are less likely to become obsolete as carriers adopt new standards.

Cell phone jamming has been tested multiple times at various prison institutions across the country, including at SCDC prisons, and has been found to be effective in preventing the use of contraband cell phones inside prisons while not blocking legitimate cell phone usage outside the covered area. In other words, the "bleed-over" which the cell phone industry claims results from jamming did not occur. I witnessed a test of a jamming system at one of our prisons and was able to use my cell phone immediately upon walking out of the cell block where the jammer was in use. During this first of its kind test, with inmates inside their cells, I was on the phone with my head of security right outside the cell block doors. I said, "I'm going in." Once I stepped through the doors, my cell phone didn't work. There was no bleed over.

As stated above, as long as there are prisons, there will always be contraband. However, contraband in the form of cell phones is one issue that can be solved if state and local prisons are allowed to block cell phone signals. Therefore, again, we are asking:

1. For a Federal Communications Commission interpretation of the Communications Act of 1934 that would permit states to use jamming technology to block the signals from unauthorized cellphones to prevent their use by prison inmates. Specifically, we are seeking an interpretation stating that signals

originating from a contraband cell phone inside of a correctional institution are not "authorized," as defined by the Communications Act of 1934. When states enact laws deeming cell phones possessed by inmates "contraband," use of such cell phones in prisons is not "authorized." Consequently, states with such laws should be permitted to use jamming technology to block the signals from these unauthorized cell phones to prevent their use by prison inmates.

2. For hearings in the Congressional committees of jurisdiction or before the Commission. This would allow sworn testimony by corrections leaders, as well as the Department of Justice, the Department of Commerce, and the wireless industry about the problem, possible solutions, and the state of jamming technology.

3. For support regarding a statutory change to allow state and local prisons to use jamming devices. There are bills pending in both chambers of Congress that would make the change (S.952/H.R. 1954, The Cell Phone Jamming Reform Act of 2019).

4. For creation of a pilot program that would allow jamming in four states and building in an evaluation component to test the effectiveness and feasibility of jamming technology.

5. For further research and testing to augment Managed Access System technology that would make such systems - which are currently highly complicated and extremely cost-prohibitive - actually work for state and local prisons.

Thank you for the opportunity to share my testimony, and thank you for your thoughtful consideration of our recommendations.

Todd Craig, MPA, MA, CPP

Chief, Office of Security Technology, FBOP

Todd Craig is Chief, Office of Security Technology, Federal Bureau of Prisons. He is responsible for the development and review of policy, audit guidelines, security-related equipment, facility design, security technology standards, security equipment testing and evaluation and a wide range of correctional security technology concerns. He serves as liaison with other federal, military, state and local law enforcement and correctional agencies, as well as the bureau's major coordinator for the development of new security technologies.

Prior to his current assignment, with over 30 years of service in the Department of Justice, Mr. Craig has served as Warden at the Federal Correctional Institution at Ray brook, N.Y., and at FCI, Beckley, W.Va. Other assignments included Associate Warden, Chief Public Information for the Bureau, and Administrator for the Federal Prison Camp in Lompoc, Calif. He received the Attorney General's Distinguished Service Award in 2018.

Mr. Craig will provide an overview of the Bureau's contraband interdiction system focusing on contraband cell phone interdiction technologies; including operational threat to Federal prisons, and current overview of managed access systems (MAS), micro jamming and the mobile MAS/seizure warrant process. Mr. Craig is a nationally recognized SME in Counter Unmanned Aircraft Systems; whole body imaging; metal detection; thermal fencing, audio-visual surveillance, wireless interdiction and synthetic drug detection. He has executed a nationwide system of contraband interdiction at 122 Federal prisons.

Educational background – Master of Public Administration – University of Southern California and Master of Arts in Criminology – University of South Florida. Certified Protection Professional (CPP) – American Society for Industrial Security.

Todd Craig, Chief, Office of Security Technology

Contraband Interdiction for the Federal Bureau of Prisons

Reduction of Crime Technology Panel:

Contraband and Cell Phones in Prison

April 15, 2020

Contraband Cell Phones in Prison

Contraband cellphones have been an ongoing correctional security and public safety concern for the Bureau of Prisons (Bureau or BOP) and state correctional systems for over a decade. Inmates use contraband cellphones to continue their illicit activities while behind bars. This criminal activity includes murder-for-hire; witness intimidation; possessing and distributing child pornography; drug trafficking; gang activity; and fraud, among other crimes. In addition to traditional detection technology used to keep contraband cellphones out of prisons, Managed Access Systems and Micro-Jamming Solutions are two viable wireless interdiction technologies that offer promising opportunities for deployment in correctional facilities. However, additional funding and authorities are required to make these technologies available for broad deployment by both the Bureau of Prisons and state correctional systems.

Scope of the Challenge and Danger

There are a number of ways that contraband cell phones get into prison, including hidden inside people and objects (for example, heads of lettuce and peanut butter jars), thrown over fences in footballs, bags and other containers, and recently and more frequently through the use of drones. One particularly troubling method is through correctional staff themselves, who are tasked with preventing this security threat. Inmates have been known to pay upwards of $1,000 for a phone. Once inmates have access to a phone, they can then use PayPal or some other payment app to directly pay inmate associates, compromised staff or contractors to continue illicit activities.

There are ongoing contraband interdiction efforts by the BOP and state prisons to keep contraband cellphones out of correctional facilities and to disable any contraband cellphones that do enter prison. To detect or prevent the introduction of contraband cell phones, whole-body imaging devices, sophisticated walk-through metal detectors and thermal fences are being used successfully for interdiction. While effective, these efforts cannot keep all contraband cellphones out of prisons, so additional methods to detect and disable contraband cell phones within prisons must be pursued. Current detection within prisons includes canine units (detect by scent) and radio frequency detection (fixed sensor and handheld units).

However, it must be kept in mind that there are issues with staff safety when physically locating and removing a cellphone. Staff resource constraints contribute to these challenges.

Despite the challenges, there are numerous factual situations and considerable past precedent that have shown the need for pursuing contraband phones as a matter of public, staff and inmate safety.

In Puerto Rico in February 2013, an 11-year veteran Correctional Officer of the Bureau of Prisons (BOP) was executed going home from work after nine inmates conspired and used contraband cellphones to orchestrate that murder. Just a year later in April 2014, a founder of the United Blood Nation (UBN) gang, incarcerated in a North Carolina facility, used a contraband cellphone to call in a "hit" on a prosecutor's father. In November 2017, the inmate was sentenced to life plus 84 months on kidnapping and related charges. The inmate was in solitary confinement at a maximum-security state facility at the time. Top state officials acknowledge that the only way he could have obtained a contraband cellphone in solitary confinement is with an employee's help.

Five years later in California, in June 2019, 16 members and associates of the Aryan Brotherhood prison-based gang were charged after a long-running Organized Crime Drug Enforcement Task Force (OCEDTF) investigation into drug trafficking and murders inside and outside of California's prisons. Nine defendants were arrested on federal racketeering and other charges for extensive, organized criminal activity, including murders, drug trafficking, and other violent crimes, all taking place from within California's most secure prisons.

At the outset of the investigation, six inmates were already serving life sentences for murder. This particular case is instructive in that criminal activity via contraband cell phone continued between 2011 and 2016. During that time, Aryan Brotherhood members and associates engaged in a variety of criminal activity, including overseeing a significant heroin and methamphetamine trafficking operation from a shared prison cell. Defendants oversaw an extensive drug-trafficking network that operated in Sacramento, Southern California, Missouri, Las Vegas, and elsewhere. As part of this continuing enterprise, contraband cellphones also allowed the defendants to communicate with other AB members and associates to direct membership in the gang, order murders (including rival prison gang members), and oversee other criminal activities.

These were by no means the only known examples, however. Several other cases also represent the challenges correctional professionals face in combatting contraband cell phones.

In March 2018, in North Carolina, 35 members and associates of the Bloods Gang pled guilty to racketeering, conspiracy, and drug trafficking and wire fraud. The Bloods Gang, part of the United Blood Nation (UBN) street gang, ultimately pled guilty to a number of charges. Those individuals who pled guilty included a "Godfather" as well as other high-ranking leaders of the organization. According to a recorded jail call, one defendant conducted gang business and participated in the distribution of gang dues while incarcerated in the New York State Department of Corrections.

In South Carolina, in June 2018, a federal inmate used contraband cellphones to lead a multi-state drug trafficking organization that distributed methamphetamine. The inmate was expected to be released in January 2019, but will now serve an additional 18 years and 3 months in federal prison for acting as the "mastermind" of a South Carolina prison meth trafficking ring. This multi-state drug trafficking organization distributed methamphetamine in the Upstate of South Carolina; Atlanta, Georgia; Kentucky; and elsewhere.

Even more recently, in Oklahoma in February 2019, white supremacist state prison gang members used contraband cellphones to operate within state prison walls planning kidnappings and other crimes that resulted in several homicides over the last 14 years. Ultimately, 18 members of a White Supremacist prison

gang based primarily in Oklahoma state prisons were charged with racketeering, drug conspiracy, and kidnapping.

To put things in perspective, consider that in 2019 the BOP recovered more than 8,000 contraband cell phones, (split between camp and secure facilities) and brought to prosecutors over 700 cases for potential criminal prosecution (78 accepted and 629 declined). In calendar year 2020, there have been 483 contraband cell phones seized in secure facilities, and 554 seized in minimum-security facilities - 1,037 phones. Ten cases have been accepted for prosecution out of 87 criminal referrals to the FBI/U.S. Attorney. Criminal referrals depend on attribution of the phone to a particular inmate. Dangerous contraband continues to be one of BOP's biggest security challenges.

Wireless Interdiction Technologies Being Tested in the Corrections Field

Two promising technologies have emerged to combat contraband cellphones in prisons: Managed Access System and Micro-Jamming Solutions.

Managed Access System (MAS) is a distributed system of radio frequency antennas that capture all cellphone signals, allowing some known signals to go through ("the whitelist") and blocking others (i.e., contraband cellphone signals). MAS is deployed by a vendor under a sub-license from a wireless carrier, captures all cellular signals within the geospatial confines of a prison and disables unauthorized cellular signals from contraband devices. MAS can be configured to provide intelligence for internal prison security and is favored by the wireless industry.

Micro Jamming Solutions (MJS) emit a signal that is stronger than the signal from the cellphone tower outside the prison, preventing cellphones from being used within the prison. MJS jams all cellular signals within the geospatial confines of a prison, but does not provide intelligence for internal prison security. The objective is to render cellular communication within the geospatial area useless.

BOP Testing of Wireless Interdiction Technologies

In calendar year 2019, BOP conducted 10 mobile MAS assessments using existing internal funds, targeting institutions with significant numbers of seized cell

phones. This technology is portable and can be relocated as needed; it is a valuable and flexible counter-measure that can be deployed quickly to react to an identified or trending contraband cell phone threat without a requirement to install expensive infrastructure.

The Bureau is also collaborating with the Department of Justice and working with the National Telecommunications and Information Administration (NTIA) on tests of MJS. As an example of how effective this technology can be, on January 17, 2018, the BOP, in collaboration with the NTIA, DOJ and the Federal Communications Commission (FCC), conducted a test of micro-jamming technology at the Federal Correctional Institution at Cumberland, Maryland. A report by NTIA affirmed positive test results.

Then again, on April 8-12, 2019, DOJ, BOP and the South Carolina Department of Corrections tested micro-jamming technology at a single housing unit within a South Carolina state prison. The test was authorized by the NTIA and coordinated with the FCC and Federal Aviation Administration. Two NTIA engineers attended the test and performed measurements of the micro-jamming equipment's radio emissions to observe and document their characteristics. BOP and DOJ staff observed that cell signals inside the housing unit were blocked, but calls outside a one-foot perimeter of the exterior could be made.

We are encouraged by the promising test results and the potential for future deployment of MJS technology.

The Bureau plans to conduct additional pilots in Fiscal Year 2020 to gauge the efficacy and cost-effectiveness of both MJS and MAS technology. This testing is mission critical, as these devices present a clear danger to prison staff, other inmates, and the public. BOP requested $4.625 million in the FY 2020 President's Budget to implement MAS and MJS pilot projects to assess the cellular interdiction technologies' capabilities. This request included funding for a proof of concept of a MAS system ($2 million) and a MJS system ($2 million) at two facilities. BOP also requested funding for $625,000 to conduct 25 mobile MAS assessments. The BOP funded each of these items in the 2020 Spend Plan.

Implementing both MAS and MJS pilots in FY 2020 will facilitate direct comparison of the wireless interdiction technologies and provide a sound roadmap for going

forward for DOJ and BOP to interdict contraband cell phones, increasing correctional institution and public safety.

State and Local Challenges

DOJ and BOP are working with federal and state partners to find ways to allow states to interdict contraband cellphones in correctional facilities. Federal agencies (like BOP) are currently permitted to jam signals at federal institutions with NTIA approval. However, state and local facilities, which house the vast majority of our country's inmates, are regulated by the FCC. And current FCC interpretation of law prevents state and local facilities from jamming signals. State and local facilities are, however, permitted to use MAS with FCC authorization.

Enhancing Safety Through Prosecution and Public Awareness

One of the challenges with reducing the number of contraband cellphones in prison is the minimal sentences handed down for possessing a contraband cellphone. Under 18 U.S.C. § 1791, providing to or possessing a contraband cellphone as a federal inmate carries a one-year statutory maximum penalty. Enhancing sentencing could have a significant impact on both the introduction and possession of contraband cellphones. One approach could be to increase the statutory maximum penalty to five years.

There is an increasing synergy of technologies used to threaten institution security and the public safety: drones and contraband cell phones. There have been a number of cases in the Bureau where drones were used by inmate associates to deliver contraband cell phones inside a prison. A recent example, at the Federal Correctional Institution, Fort Dix, New Jersey, on March 12, 2020, at approximately 7:45 p.m., staff observed an unmanned drone flying over the compound. As staff approached the area, they discovered an inmate with a bag around his torso containing 34 phones, six hands free headsets, 9 chargers, 51 SIM cards, and 3 64 GB SD cards. The inmate responsible was placed in the Special Housing Unit, pending criminal investigation.

In summary, contraband cell phones are a significant security challenge to our prison system. While often not fully appreciated, contraband cell phones can result in ongoing criminal enterprise, injury, and even death to both our staff and

inmates. Further, they are a continuously evolving challenge and threat. To counter the threat, the BOP must continuously evolve adapt and learn, which we do every day and from every incident.

Next Steps - Specific Recommendations to the Commission:

The Commission can take the following actions to support correctional staff in combatting contraband cell phones:

1. Recommend the NTIA and the FCC support spectrum use requests from correctional agencies to deploy MJS, MAS and Mobile MAS technologies.
2. Recommend Federal, state and local legislatures fund these contraband cellular interdiction technologies, including micro jamming, as a matter of public safety, as well as statutory changes to effectuate deployment of those technologies.
3. Recommend the wireless industry cooperate with corrections and law enforcement in developing low cost, innovative wireless interdiction technologies to ultimately remove the threat of contraband cell phones from the over 7,000 Federal, state and local jails and prisons across the United States.

Thank you for the opportunity to share my testimony and considering these recommendations.