U.S. DEPARTMENT OF JUSTICE

President's Commission on Law Enforcement and the Administration of Justice

Reduction of Crime Hearing

April 14 - April 16, 2020

TABLE OF CONTENTS

Reduction of Crime Hearing Teleconferences

- **Tuesday, April 14th, Hearing 2:00pm to 3:00pm, Eastern Time – Domestic Violence and Sexual Assault**
  - Matthew Gamette, Director of Forensic Services, Idaho State Police
  - Kim Garrett, CEO, Palomar, Oklahoma City's Family Justice Center
  - Richard Hertel, Prosecutor, Ripley County, IN
  - Robert Hawkins, Chief of Police, Muscogee Creek Nation

- **Wednesday April 15th, 4:00pm to 5:30pm, Eastern Time –Technology Issues Encountered by Law Enforcement**
  - Darrin Jones, Executive Assistant Director for Science and Technology, FBI
  - Cyrus R. Vance, Jr., District Attorney, New York County, NY
  - Chuck Cohen, Vice President, The National White Collar Crime Center
  - Bryan Stirling, Director South Carolina Department of Corrections
  - Todd Craig, Chief, Office of Security Technology, Federal Bureau of Prisons

- **Thursday, April 16th, Hearing 2:00pm to 3:00pm, Eastern Time – Leveraging Technology to Reduce Crime**
  - Tom Ruocco, Chief of Criminal Law Enforcement, Texas Department of Public Safety
  - Chief Bill Partridge, Oxford, AL Police Department
  - Christopher Amon, Chief of Firearms Operations Division, Bureau of Alcohol, Tobacco, Firearms and Explosives
  - David LeValley, Deputy Chief, Detroit Police Department

Tuesday, April 14, 2020

Matthew Gamette

Director, Idaho State Crime Lab

Mr. Gamette was born and raised near Salt Lake City, Utah. He attended college at Brigham Young University in Provo, Utah and did undergraduate work in Zoology. He also received a Master's Degree from Brigham Young University in Microbiology where he studied parasitology with an emphasis on *Plasmodium falciparum* malaria. Mr. Gamette completed a certificate program in laboratory management through West Virginia University Forensic Management Academy, holds a certificate in Laboratory Management and Leadership from the University of California at Davis, and graduated as a Certified Public Manager in the Idaho program.

Mr. Gamette interned with the Utah State Crime Lab in Salt Lake City, Utah. He worked in the Spokane Laboratory of the Washington State Patrol from 2002 to 2008 as a biologist/DNA scientist and crime scene responder. He was promoted to Forensic Scientist 4 (Spokane Local DNA Technical Lead) in 2008. He has trained hundreds of detectives, crime scene responders, forensic nurses, and first responders in the collection of biological evidence. Mr. Gamette started his career with the Idaho State Police in late 2008 as the Laboratory Improvement Manager/Quality Manager for the laboratory system. He was promoted to Laboratory System Director over the three laboratories of the Idaho State Police in July 2014.

He serves as the ASCLD representative on the Consortium of Forensic Science Organizations (CFSO) and has served as the Chair of the CFSO Board for several years. Mr. Gamette served as an elected board member of the American Society of Crime Lab Directors (ASCLD) for over seven years and served as President from 2018-2019. He Chaired or Co-chaired several ASCLD committees including Finance, Symposium Planning, Advocacy, the Sexual Assault Kit Task Force, and the ASCLD Accreditation Initiative. He currently serves as the Co-chair of the ASCLD Advocacy Committee and leads the ASCLD Accreditation Initiative. He was a certified assessor with the American Society of Crime Lab Directors-Laboratory Accreditation Board (ASCLD/LAB), and has performed DNA laboratory assessments all over the United States as a certified FBI DNA assessor. He is also an audit panel reviewer for the FBI's National DNA Index System (NDIS). He was selected and served a five year term on the NIST Organization of Scientific Area Committees (OSAC) Quality Infrastructure Committee (QIC). He currently serves as an affiliate OSAC member on the FSSB Terminology Task Group. He was selected by the US Department of Justice to participate as a member on the Forensic Laboratory Needs-Technology Working Group (FLN-TWG) where he currently serves. He is a member of the editorial board for the prestigious journal Forensic Science International-Synergy. He is a member of the American Academy of Forensic Sciences (AAFS), Northwest Association of Forensic Scientists (NWAFS), American Society of Crime Lab Directors (ASCLD), and Association of Forensic Quality Assurance Managers (AFQAM).

Written Testimony of Matthew Gamette
Presidential Commission on Law Enforcement and the Administration of Justice
April 14, 2020

My name is Matthew Gamette and I am the Laboratory System Director for the Idaho State Police Forensic Services. I oversee a laboratory system with three regional laboratories and over 50 scientists and staff. I currently Chair the Consortium of Forensic Science Organizations (an organization representing over 21,000 forensic science practitioners) and am Immediate Past President of the American Society of Crime Laboratory Directors. I have worked as a forensic scientist for 18 years. I will make recommendations for how labs and law enforcement can work more collaboratively on domestic abuse and sexual assault investigations and focus on four key areas of recommendations.

Resources:

The first key area is meeting the resource needs of forensic providers. Forensic labs provide investigative information, identify and bolster cases against perpetrators, and exonerate the innocent. This work requires ample operating budgets, sufficient personnel, and adequate facilities. As identified in the NIJ 2019 Forensic Laboratory Needs Assessment Report to Congress, Forensic Science Service Providers (or FSSPs) would require a minimum of an additional $640 million annually to balance the present number of incoming laboratory requests with reports issued from the lab. I recommend that the President's budget make an even greater financial investment in forensic science. Grants such as Coverdell, and the DNA backlog reduction and efficiency grants (CEBR) must be authorized and appropriated at higher levels, and traditional grants made available to law enforcement, such as Byrne JAG, should be increased and made more available to forensic labs. Law enforcement investigators need more access to forensic labs and disciplines. We are losing the ability in this country to perform forensic examinations such as trace analysis because they are expensive. As a result, investigators in many instances are not trained to collect these types of evidence and courts do not have the opportunity to consider all evidence that may have been available during an investigation. If evidence is not collected, forensic analysis is not needed. If forensic analysis is not requested by law enforcement, the lab cannot justify having or keeping the examiner and the equipment. If labs do not have examiners in a particular discipline, the officers are either not trained to collect the evidence or are asked not to collect the evidence because it cannot be examined without committing significant resources to a private contractor. This is a vicious cycle leading to the extinction of helpful forensic disciplines as well as not availing the court to all evidence in deliberating the guilt or innocence of an individual. I recommend not only funding of instrumentation and personnel for these withering forensic disciples, but the creation of national training centers and programs to ensure uniformity

across the country of properly qualified forensic examiners. I recommend comprehensive forensic evidence collection and packaging training programs for law enforcement taught by forensic science practitioners. Forensic scientists can instruct officers during POST initial training, POST continuing education, and through partnerships like the OJP funded Regional Information Sharing Systems (or RISS network). This spring ISPFS trained 200 officers in DNA techniques and technology by partnering with the Rocky Mountain Information Network (part of the RISS network). Officers may not recognize or collect critical Domestic Violence or Sexual Assault Evidence if they are not trained to recognize, properly document, and collect such items. We must improve the training of officers regarding what services their forensic lab can provide and how the technology can help their investigation. I respectively recommend that as technology continues to be transferred to law enforcement field applications, forensic scientists must collaboratively partner with law enforcement for training and implementation. The most successful and quality applications of field instrumentation for drug detection, DNA, and breath alcohol are highly coordinated with the forensic scientists for quality, reliability, and scientific validity. The National Institute of Justice Forensic Laboratory Needs Technology Working Group (FLN-TWG) is an excellent resource the federal government has to transfer technologies developed by military or federal agencies to state and local forensic science practitioners. Further, I recommend leveraging federal and state cooperative groups to ensure that validation work is completed in advance of instrumentation purchases. Collaborative validations and procurement is a benefit to large and small forensic science providers. FSSPs could very much benefit from having a program like the one the CDC has set up in the "Public Health Crisis Cooperative Agreement." Under this model, validated instrumentation can be set at a price point for the forensic laboratories to obtain, rather than making each lab do the procurement and validation work. The forensic science laboratory system in the country should be looked at like the CDC Laboratory Response Network (LRN) where there can be more collaboration between states for validation studies and more ability to scale up resources for emergency or critical response capability. Right now, it is difficult for labs to set up MOU agreements to share resources such as one lab with greater capacity working cases for a lab with limited capacity. I recommend that we develop easier ways for law enforcement to ask questions of the lab scientists in real time. This requires both cultural change for officers and scientists to be comfortable talking to each other and technology to allow for the immediate communication. There are often large cultural differences between the scientists in the lab and the law enforcement officers. They are trained and educated very differently. Breaking down the communication barriers and getting them to work together in real time to solve investigative challenges is the best way to operate. At ISPFS, we are working on ways to encourage the law enforcement officers to call the scientists on their desk phones or work cell phones to ask questions about evidence collection or processing.

Backlogs are real and require resources. Right now in this country, according to Dr. Paul Speaker and Project Foresight, the published data demonstrates that for every 1% reduction in turnaround time at the lab, there is a 1.29% increase in cases submitted to the lab and a 3.9% increase in the number of items submitted to the lab. To solve DNA backlogs we need more forensic scientists, bigger facilities, and funding. Turnaround time is directly proportional to forensic lab staffing. Increased staffing requires bigger laboratory facilities. The National Institute of Standards and Technology (NIST) recommends a facility of 700-1000 square feet per forensic analyst to allow for adequate workspace. Most modern state and local forensic science laboratories have analysts crammed into all available space including closets and utility spaces. Continually adding new staff to address backlogs without addressing the laboratory facility capacity will lead to bottlenecks and not backlog reduction. I respectfully recommend using tools like the National Institute of Justice/West Virginia University/Forensic Technology Center of Excellence FORESIGHT workforce calculator tool that calculates how many staff are needed to produce a desired turnaround time. Project FORESIGHT also helps forensic laboratories become more efficient by self-evaluation of efficiency metrics and allows leaders to share information with each other about techniques to increase laboratory efficiency. Getting better lab turnaround time speeds investigations and reduces recidivism. Controlling backlogs also requires controlling intake. I recommend evaluating submission policies with labs collaboratively to determine what is actually necessary for an investigation and subsequent prosecution. I cannot emphasize enough the importance of meeting in triage teams with the lab, investigators, and prosecutors participating collaboratively in the evidence selection process. A paramount recommendation is the development of electronic data exchange between law enforcement, the lab, and court case management systems. Labs need to know, through automated means, when cases are no longer being investigated or prosecuted. This knowledge allows labs to stop work on unnecessary cases and move on to the next critical case. The technology exists for court and law enforcement customers to know lab case status in real time. This technology should be more widely implemented. Lab customers should also be able to electronically review and print lab case reports and notes immediately after the case is complete without having to call the forensic scientist or laboratory.

Sexual Assault Response Collaboration:

The second set of recommendations is for sexual assault response collaboration. I respectfully recommend each state have additional resources and effort dedicated to diverse state working groups. In Idaho, we have the Idaho Sexual Assault Kit Initiative (ISAKI) group that meets several times a year to determine state policies, training needs, and potential state laws. This is a highly collaborative group working to make collection, treatment of victims, law enforcement, and prosecution even better in our state. Each state needs more trained Sexual Assault Nurse

Examiners (SANE) and more training available for these nurses after they are initially trained. Trained medical personnel must collect sexual assault evidence to maintain the evidentiary value of the kit and give the lab the best evidence. There must be more training and support for state and local Sexual Assault Response Teams (SART) with heavy engagement from labs and law enforcement. I recommend more federal resources to train Sexual Assault Nurse Examiners (SANE) and funding for state level SANE/SART coordinators to help the local programs. Every state should have a mechanism to notify survivors of their kit location and testing status. Each state must have a sexual assault kit tracking system with input by collection nurses, law enforcement, and labs. Idaho has pioneered kit tracking with the first fully implemented statewide kit tracking system in the country (IKTS). To help other entities embrace kit tracking policy, Idaho makes this kit tracking software available free to any public entity. The Bureau of Justice Assistance (BJA) Sexual Assault Kit Initiative (SAKI) granting program also makes funds available for entities to procure sexual assault kit tracking software and implement it in their jurisdiction. Each state must perform an independent audit of how many kits they have, where they are located, and the lab testing status. At least 60,000 kits still exist in the US that have not been submitted for testing. Laws for kit collection, testing, and retention in many states are confusing for law enforcement and forensic labs. Labs are often required to decide if it is appropriate to test a kit when federal law protects the right of a survivor not to report a crime, yet some state laws still require kit testing. The lab should be the arbiter of law, potentially violating either state or federal statute. I recommend national standardization of the kits to SAFER working group recommendations to eliminate state-to-state variation of kit components. We must consider all forensic disciplines, like standard toxicology testing for drug-facilitated sexual assault, not just DNA. Every forensic discipline could play an important role in investigating a sexual assault and should be considered when thinking about a holistic approach to kit testing. For productivity and speed, labs are processing kits for DNA in an assembly line format or outsourcing kits to private labs. Most labs are limiting the samples tested per kit. We must develop public lab infrastructure to process all kits, test all probative evidence in each kit, and ensure each eligible sample is entered in CODIS. CODIS entry can only be done in public labs. Finally, I recommend a more robust documentation of law enforcement actions to follow-up and resolve CODIS hits generated by labs. Far too often, these hits are not investigated due to a lack of resources or other communication obstacles.

Forensic Criminal Intelligence Sharing:

The third set of recommendations is criminal intelligence. Forensic labs have an incredible amount of actionable and time relative data. The recommendations of the recent OJP report on promising practices in forensic lab intelligence should be highly considered. Data is available that is not being leveraged to predict emerging drug threats, gun crime, DUI driving trends, etc. I

recommend focus groups to develop infrastructure to share this data from labs with fusion centers, HIDTAs, and state and federal agencies. Labs play a critical but mostly unexplored role in criminal intelligence.

Quality Assurance, Risk Management, Accreditation, and Certification:

The fourth set of recommendations is related to quality assurance and risk management. Federally, prosecutors are now required to use an accredited lab for analysis if one exists for the purpose of the analysis. Accredited forensic science laboratories are required to follow strict management and analytical policies and procedures, providing a level of confidence to the courts of good scientific practice. Since the vast majority of forensic science is performed in the nation's state and local law enforcement agencies, this Commission should recommend that states require accreditation of forensic providers and certification of forensic scientists. This includes recommending funding to educate, train and competency test all forensic practitioners. Part of accreditation is implementation of evolving international and national standards into lab protocols. Of particular concern is accreditation in the growing world of digital forensic laboratories that are critical in the investigation and prosecution of domestic violence and sexual assault cases. Finally, this Commission should recommend more federal research and development funding and a federal research strategy for forensic science in the United States. Most forensic science laboratories cannot do foundational or applied research or technology transfer. More must be done on the federal level to support the practice of forensic science. The federal government must support foundational research and find more efficient ways to implement validated technologies in the laboratory. Research and development has been a great benefit to investigate sexual assault and domestic violence cases. The implementation of DNA and CODIS in the last 30 years, and the emerging fields of forensic molecular genealogy, full genome sequencing, and proteomics resulted from research and development. Research and development in other areas of forensic science are equally important to generate instrumentation and techniques that are faster, increasingly sensitive and more discriminating.

Forensic science, as performed by forensic service providers every day, is a critical element in the administration of justice across the United States. Whether it is assisting to identify and convict the guilty, exonerate the innocent, or give closure to a victim of a crime and their family, the citizenry served by the forensic science expects and deserve the most current, valid, and reliable forensic science.

I appreciate your attention and the time you have afforded me to present and respectfully ask you consider these important issues.

Appendix A
Recommendations

Resources:

- Data sharing mechanisms for case management systems at LE/Lab/Courts to update case status
- On demand electronic lab case updates, reports, and case information available for customers
- President's budget needs to make an even greater financial investment in forensic science
- Higher authorization and appropriation in Coverdell, CEBR, and Byrne JAG for FSSPs
- Funding for laboratory instrumentation in trace disciplines
- National training centers for workforce development in all forensic disciplines
- Training for officers in all forensic science disciplines for evidence recognition and collection by forensic scientists coordinated through police training entities
- LE and lab joint technology implementation committees for forensic science in states and localities
- Federal CoAg groups for technology procurement, validation, and implementation
- Forensic Science Laboratory Response Network agreements for validation and resource sharing
- Direct communication for officers doing investigations to talk to laboratory scientists in real time
- Develop a model to "right size" forensic services in an area (lab size, instruments, and staff) given crime data rates and jurisdiction population.
- Enhanced calculators to determine appropriate number of analysts for caseload and turnaround times
- More federal resources for state and local entities to build and expand forensic science facilities

Sexual Assault Response Collaboration:

- More resources for follow-up collaboration and accountability on CODIS hits
- Federally supported diverse state sexual assault response working group in every state
- More federal support for state and local Sexual Assault Response Teams (SART) and SANE/SART coordinators and trainers in every state
- More federal support and resources for Sexual Assault Nurse Examiner (SANE) training
- Sexual assault kit tracking system or mechanism in every state or location
- Independent sexual assault kit audit in every state to determine actual scope of kit testing needed
- Federally coordinated sexual assault kit components to SAFER recommended guidelines
- More resources for collection and forensic testing for drug facilitated sexual assault
- Standardized recommendations for processing and testing sexual assault kits
- Clarification of VAWA for the testing of Jane/John Doe kits

Forensic Criminal Intelligence Sharing:

- Federal working groups and funds focused on forensic intelligence data sharing and collaboration
- Implementation of recommendations in OJP Promising Practices in Forensic Laboratory Intelligence

Quality Assurance, Risk Management, Accreditation, and Certification:

- Accreditation of all forensic science labs and certification of all forensic science practitioners
- Required training, competency testing, and continuing education for every forensic science practitioner
- Federal forensic science research strategy and funding for federal research and development

Appendix B
Reference Hyperlinks

https://nij.ojp.gov/library/publications/report-congress-needs-assessment-forensic-laboratories-and-medical

https://bja.ojp.gov/funding/opportunities/bja-2020-18434

https://bja.ojp.gov/program/jag/overview

https://www.riss.net/centers/rmin/

https://www.riss.net/

https://nij.ojp.gov/topics/articles/forensic-laboratory-needs-technology-working-group-opening-new-channel-improve

https://www.cdc.gov/cpr/readiness/funding-crisis.htm

https://www.cdc.gov/cpr/readiness/funding-crisis.htm

https://www.justice.gov/ncfs/page/file/958466/download

https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7941.pdf

https://forensiccoe.org/workforce-calculator-project/

https://business.wvu.edu/research-outreach/forensic-business-studies/foresight

https://isp.idaho.gov/SexualAssaultKitTracking/

https://bja.ojp.gov/program/sexual-assault-kit-initiative-saki/overview

https://www.sciencedirect.com/science/article/pii/S2589871X19301627

https://www.justice.gov/ovw/page/file/931391/download

https://www.ncjrs.gov/pdffiles1/nij/250384.pdf

https://it.ojp.gov/GIST/1211/Promising-Practices-in-Forensic-Lab-Intelligence

https://www.justice.gov/opa/pr/justice-department-announces-new-accreditation-policies-advance-forensic-science

Kim Garrett

CEO and Founder of Palomar: Oklahoma City's Family Justice Center

Kim Garrett, LMSW, NACP, is the CEO and founder of Palomar: Oklahoma City's Family Justice Center, a successful collaborative that brings agencies together to help victims of crime. Kim has passionately worked in victim services for 18 years and is nationally certified as an Advanced Advocate through the National Organization for Victim Assistance (NOVA). Kim established Oklahoma City Police Department's Victim Services Program in 2011 which later received Honorable Mention for Excellence in Victim Services from the International Association of Chiefs of Police. In 2013, Kim received a Commendation for Victim Services from Governor Mary Fallin and in 2017 she was the first civilian to receive the Medal for Meritorious Honor from Oklahoma City Police Deptartment. In April 2018, Palomar was recognized by the Department of Justice for innovation and building strong partnerships. Most recently, Kim began consulting with the Alliance for HOPE International to help build Family Justice Centers. Kim serves on Governor Stitt's Criminal Justice RESTORE Task Force and nationally for the Office for Victims of Crime Technology Initiative. Kim is proud to be working alongside amazing partners, survivors and visionaries to change the framework for survivors and their children in Oklahoma City. Kim is a proud mother to two amazing children, Deacon (9) and Olive (6) and has been happily married to her husband Bob for 11 years.

Palomar
OKLAHOMA CITY'S FAMILY JUSTICE CENTER

A PROJECT WITH THE CITY OF OKLAHOMA CITY

Kim Garrett, CEO and Founder
Palomar: Oklahoma City's Family Justice Center
Reduction of Crime Hearing
Enhancing the Criminal Justice System's Response to Domestic Violence and Sexual Assault
April 14, 2020

The Problem

The impact of domestic violence is significant and profound. In the United States, an average of 20 people experience intimate partner physical violence every minute. This equates to more than 10 million abuse victims annually[i]. In 2018, Harvard declared domestic violence in the United States as a public health epidemic[ii].

You cannot have safe communities if you do not have safe homes.

Domestic violence crimes have a tremendous fiscal impact on law enforcement agencies. A conservative estimate in Oklahoma City (2016) showed a fiscal impact of $9,056,163 for dispatch, patrol, crime scene investigation, homicide, detectives and more. On a national level, the Centers for Disease Control and Prevention have found domestic violence costs the United States over $5.8 billion dollars annually, with 70% representing care and mental health expenses as a result of the crime.[iii] While those costs are significant, it does not include: housing, incarceration, social services and the long-term impact on children. All of which have a lasting effect on our agencies, public safety, and our nation.

Seventy-five percent of children who witness domestic violence will grow up to repeat the same behavior[iv]. If one person in a family chooses to use violence and control, within four generations, 18 people will continue the cycle. Generational violence is multiplying exponentially and it's too big of an issue for any one profession to combat alone, ***we've got to come together to improve outcomes***.

The Family Justice Center model began in San Diego in 2002 and quickly grew into a best-practice and evidence-based model[v]. To date, there are over 130 Family Justice Centers across the US and many developing around the world. The Family Justice Center model is victim-centered and brings all services into one convenient location, reducing barriers and increasing access for families to receive a variety of services.

Research consistently shows when diverse professions work together through a collective impact model, it yields better outcomes. In that spirit, Oklahoma City Police Department took the lead on a bold new vision for increasing public safety. OCPD brought agencies together, under one roof, to form the first integrative collaborative in our community [vi]to help victims of domestic violence, sexual assault, stalking, elder abuse and human trafficking. Now affectionately known as Palomar: Oklahoma City's Family Justice Center.

Law enforcement's leadership was directly related to our level of success.

Prior to our development of a collaborative model in 2015, many of these professionals had never worked together, or even met, despite working the same cases. For example, the child welfare workers had never interfaced with the domestic violence Detectives, and Law Enforcement Advocates had not worked with civil/legal attorneys. Agencies were giving victims brochures and mainline phone numbers for them to coordinate services on their own, and families were unintentionally falling through the cracks. Our collaborative model brought together diverse professionals such as:

- State partners including: Prosecutors, Child and Adult Welfare, Mental Health
- City and County partners such as: local police departments, Sheriff's office, Animal Welfare
- Federal partners including: US Attorney's Office, US Marshals, ATF
- Dozens of Nonprofits who provide a myriad of services including: advocacy, civil/legal assistance, food and basic needs, childcare, therapy, shelter, parenting classes, support groups, medical and forensic services, pet therapy and advocacy and more.

While family crimes are typically treated as separate entities (separate units for DV, SA, CA/N) these crimes are often committed by the same offenders. Co-occurrence is significant, meaning the same person abusing his wife, is also committing other crimes such as: child abuse, elder abuse and animal abuse.

In FJC's, gaps in service(s) are easily identified and remedied with a coordinated response in real time. Partners have said what used to take seven weeks of coordinating between professionals, now takes seven minutes, thanks to physically working in the same location. High Risk Team Meetings are conducted regularly as needed to prioritize high risk cases, ensuring a rapid collective response to cases with the highest lethality potential. In return, victims feel safe, have increased satisfaction and are healing faster because of the myriad of wrap-around services we are able to provide.

Measuring Success

The outcomes we've seen to date are undeniable:

- Improved relationships with agency partners, and an expansion from 14 to 34 agencies!

- With on-site forensic exams and support services for survivors, Detectives have improved case work. To quote our District Attorney, "Cases are demonstratively better" with an increase of 38% of cases being filed. (David Prater, 2018)
- 8.4% reduction in domestic related calls to 911
- 80% reduction in children in homes with domestic violence being placed into the child welfare system
- Lives saved. For the past 20 years, Oklahoma has consistently ranked in the top ten worst states for Women Murdered by Men[vii]. In 2011 we ranked 3rd, In 2013 we ranked 6th and in 2018 we went down to 20th. **Oklahoma's best ranking ever.**

Recommendation #1: Prioritize federal funding for Family Justice Center Models

Funding for operations and administration of this private/public model is essential to ensure sustainability for collective impact programming. When service providers can sit at the same table and discuss a case, you collectively develop new options, improve standards of care, and increase offender accountability. Family Justice/Multi-Agency models need to be elevated as a priority for long-term federal funding. It would be ideal to develop funding opportunities specifically for multi-agency teams within a FJC to create new positions including: prosecutor (cross deputized through the US and County Prosecutor), therapist, civil/legal attorney, detective and advocate. This would take budgetary pressure off the leadership and allow for more creativity and innovation in solving these cases in their respective communities.

Recommendation 2: Develop Shared Consent to Share Information

For victims who choose to get wraparound services in a collaborative model, there should be the option of shared consent. Current federal funding policies and rules are not written in consideration of collaborative and integrative models. At the same time, while federal funding requires many agencies to collaborate, they have direct policies preventing or greatly restricting information sharing. All federal funding for victim service providers: Violence Against Woman Act (VAWA), Victims of Crime Act (VOCA), Family Violence Prevention and Services Act (FVPSA) requires a coordinated community response to sexual assault, domestic violence, dating violence, and stalking. The law asks jurisdictions to bring together stakeholders from diverse backgrounds to share information and use their distinct roles to improve community responses to violence against women.

The VAWA Confidentiality Provision refers to 34 U.S.C. 12291(b)(2), a provision that requires all grantees receiving VAWA funding from the Department of Justice, Office on Violence Against Women, to protect the confidentiality and privacy of persons to whom those grantees are providing services. This Provision is designed to ensure the safety of adult, youth, and child victims of domestic violence, dating violence, sexual assault, and stalking. (U.S. Department of Justice, Office on Violence Against Women)

Any agency receiving VAWA or FVPSA funds must adhere to this confidentiality. By statute, a grantee may share personally identifying information in three specific circumstances[viii]:

(1) When the victim provides written, informed, and reasonably time-limited consent to the release of information ("a release");
(2) When a statute compels that the information be released; or
(3) When a court compels that the information be released.

A victim's confidentiality is of utmost importance. However, the governments mandate to collaborate and its stance related to extreme confidentiality in correlation with funding programs, creates an incongruency in policy that hamstrings collaborative models from proving holistic services. Furthermore, there are entities who prefer the status quo, use these policies to stifle collaboration and are advocating for even stricter requirements, despite survivors' frustration.

When you think about the dynamics of domestic violence, clients usually reach out during crisis and in desperation. They are fleeing for their safety, fearful they could lose their children, sometimes healing from physical injuries, and oftentimes experiencing PTSD inducing trauma. Is it realistic for professionals to expect victims to be able to anticipate what information will need to be shared, with whom and for how long?

Recommend the Federal level develops a task force of diverse leaders from professions who regularly interface with crime victims (law enforcement, attorney, medical, advocate, therapy, a survivor, etc.) and work together to develop a shared Informed Consent for collaborative models. There are ways to responsibly share information within a collaborative, while also providing informed consent and honoring the client's confidentiality. Policy needs to adapt to today's current needs.

In domestic violence situations, time and access to services can literally be the difference between life and death. We need to consider expanding consent to include verbal consent (digitally recorded, etc.). Further, develop technology or a platform for professionals to get consent electronically and responsibly share information with the victim's consent. For example, we recently had a triple homicide in our state. ATF was reaching out to advocates to see if the victim disclosed anything that could be helpful in their investigation. Advocates could not have predicted this request and since they did not specifically have a release for ATF, and since the victim was murdered, they could not consent to information sharing. The only way for them to get the information now would be through a court order.

To maximize the tools of integrated services, consider expanding consent to share relevant information with the victim's consent, among designated professionals within a collaborative working with the same client/case. For instance, consider hospitals: You don't have to sign a written consent form when transported by ambulance, nor do you have to sign one each time you interact with a different medical professional, get lab work done or medical scans. Build shared consent that works with a professional integrated model.

Our current system, while well-meaning, is inefficient for survivors' who want to engage with collaborative models and has created unintended consequences and barriers. When survivors must sign five different consent forms each visit to a collaborative model, it becomes overwhelming, frustrating and is not the best use of anyone's time.

Recommendation #3: Increase Federal Resources to Support State Efforts in Combating Domestic Violence through Project Safe Neighborhood (PSN)

Within our collaborative, we recognized early on to achieve victim safety, you must also partner with agencies who enforce offender accountability. Oklahoma County has a high prosecution caseload with 1,800 domestic cases being filed in 2018, but only had three Prosecutors and one Supervisor. Further, offenders were bailing out on state charges and waiting 1-2 years for court. We decided to expand our partnerships to a federal level and reached out to the U.S. Attorney's Office, Western District in May 2018.

The U.S. Attorney's office found Title 18: section 922 which federally prohibits domestic violence abusers who are subject to a victim protective order or have been previously convicted of a misdemeanor crime of domestic violence from possessing a firearm. This is significant as the presence of a gun in a domestic violence situation increases the risk of homicide by 500%[ix].

At the same time, the U.S. Attorney's Offices were tasked with revitalizing Project Safe Neighborhoods (PSN)[x], a grant to reduce violent crime. "Operation 922" was born and brought together AUSA's, ATF, US Marshals, local law enforcement, State Prosecutors and non-profit advocates to prioritize firearm prosecutions connected to domestic violence.

In 2018, The U.S. Attorney's Office used PSN funds to pay for a State Prosecutor who was cross deputized as a AUSA. In 2019, the PSN grant was used to cross-designate a law enforcement officer with ATF. Partners meet weekly to staff cases. Outcomes to-date include: 99 cases charged, 85 guilty (convictions or pleas), average sentence is 81 months, 35% of convicted were known gang members. There have been 153 firearms seized and over 3,000 rounds of ammunition.

There are dozens of success and lives have been saved because of this partnership. Not only for victims of domestic violence and their children, but for police officers as well. Since federal entities can move for detention immediately until trial, defendants are not able to bail out and harass, intimidate or injure their victims. Further, since the prosecution is based on possession of the weapon, you don't need to have a victim cooperate or testify. It reduces their trauma while simultaneously increasing their safety.

I recommend increasing federal resources to support state and local efforts and address domestic violence through Project Safe Neighborhoods. This creative collaborative can reduce domestic violence and gun violence while simultaneously enforcing federal firearms laws.

Thank you for your time and consideration of these recommendations. If you have questions or would like more information, please feel free to contact me at 405.552.1010 or via email at: Kimberly.garrett@okc.gov

Resources

[i] Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J. & Stevens, M. (2011). The national intimate partner and sexual violence survey: 2010 summary report. Retrieved from http://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf. 2 National Center for Injury Prevention and Control, Centers for Disease Control and Prevention (n.d.). Infographic based

[ii] Valera, E. (2018). Harvard Health Publishing, Harvard Medical School. Intimate partner violence and traumatic brain injury: An "invisible" public health epidemic. Retrieved from: https://www.health.harvard.edu/blog/intimate-partner-violence-and-traumatic-brain-injury-an-invisible-public-health-epidemic-2018121315529

[iii] National Center for Injury Prevention and Control. Costs of Intimate Partner Violence Against Women in the United States. Atlanta (GA): Centers for Disease Control and Prevention; 2003. Retrieved on April 13, 2020 from: https://www.cdc.gov/violenceprevention/pdf/ipvbook-a.pdf

[iv] Crime Victims Institute, 2013

[v] Violence Policy Center, When Men Murder Women: An Analysis of Homicide Data. Published reports from 1998 – 2018.

[vi] Hellman, C.M., Gwinn, C., Strack, G., Burke, M., Featherngill, J., Aguirre, N., & Aceves, Y. (2017). Survivor Defined Success, Hope and Well-Being: An Assessment of the Impact of Family Justice Centers. Retrieved on April 13, 2020 from: https://www.acesconnection.com/fileSendAction/fcType/0/fcOid/475599658395137170/filePointer/475599658395163665/fodoid/475599658395163652/FJC%20OU%20Report.FINAL.pdf

[vii] Violence Against Women Act: Confidentiality Provision (34 U.S.C. § 12291(b)(2)) | 3

[ix] Risk Factors for Femicide in Abusive Relationships: Results From a Multisite Case Control Study. Jacquelyn C. Campbell, Daniel Webster, Jane Koziol-McLain, Carolyn Block, Doris Campbell, Mary Ann Curry, Faye Gary, Nancy Glass, Judith McFarlane, Carolyn Sachs, Phyllis Sharps, Yvonne Ulrich, Susan A. Wilt, Jennifer Manganello, Xiao Xu, Janet Schollenberger, Victoria Frye, Kathryn Laughon. Am J Public Health. 2003 Jul; 93(7): 1089–1097.

[x] United States Department of Justice, Project Safe Neighborhood (PSN): Revitalized in 2018. Retrieved on April 14, 2020 from: https://www.justice.gov/usao-wdok/project-safe-neighborhood-psn-revitalized-2018

Richard J. "Ric" Hertel

Ripley County Prosecuting Attorney

Mr. Hertel is the elected Prosecuting Attorney in Ripley County, the 80th Judicial Circuit in Indiana. He was first elected in 1998. Prior to becoming Prosecutor, Mr. Hertel did criminal defense work. He presents regularly to State, County, and Local police agencies on a variety of different topics including 4th Amendment, domestic violence, OWI law, sexual assault, and updating officers on changes in statutory and case law. He has presented for the *Indiana Prosecuting Attorney's Council (IPAC)* and is currently on the Board of Directors of the Association of Indiana Prosecuting Attorneys Inc., an organization representing Indiana's prosecutors. He has acted as faculty at the *National Advocacy Center* and for the *National District Attorney's Association (NDAA)* throughout the country on various topics, including trial advocacy, sexual assault, domestic violence, ethics, community prosecution, *Crawford*, prosecuting public figures, and civil liability. In 2012, Mr. Hertel taught for the *National Children's Advocacy Center* at the *28th Annual National Symposium on Child Abuse* in Huntsville, AL. He also presented in 2013 in Dallas at the *25th Annual Crimes Against Children Conference* on the Multidisciplinary Team. In 2019, Hertel presented at the Crimes Against Women Conference in Dallas on a newly created topic, The Kavanaugh Effect. Additionally, he has taught for state prosecutor organizations in Idaho, Arkansas, Montana, and Kentucky. He has presented for the *Indiana Coalition Against Domestic Violence (ICADV), Rape Task Force of Fort Wayne, Marion County Prosecutor's Office* and the *Dekalb County Domestic Violence Task Force*.

In 2003, Mr. Hertel received the "Benjamin Harrison Award" as Indiana's outstanding elected official. That same year he was also awarded the "Friends of Safe Passage Award" for his work with victims of domestic violence. In 2007, the Indiana Coalition Against Domestic Violence named him Outstanding Prosecutor of the year. He was instrumental in starting the Region 15 CAC, Indiana's first regional CAC that serves six rural counties, including his. Mr. Hertel currently serves on the CAC's board of directors.

Written Testimony of Richard J. ("Ric") Hertel
Prosecuting Attorney, Ripley County, Indiana
April 14, 2020

The Impact of Domestic Violence and Sexual Violence on Law Enforcement and The Administration of Justice

My remarks today are based on my time as a defense attorney and 21 years of service as the elected prosecutor in Ripley County, Indiana. During my tenure as Prosecuting Attorney, I developed best practices for law enforcement in my community, personally handled domestic and sexual violence cases, and trained prosecutors handling sexual and domestic violence cases across the country. These experiences showed me the gaps in our justice system's response to domestic and sexual violence crimes, and have led me to advocate for new and better law enforcement strategies over the course of my career.

Left unaddressed, offender-victim dynamics in cases of domestic violence threaten victim safety, compromise victims' ability to participate in the criminal justice process, and impact the type and availability of evidence that can be used to prosecute offenders.[1] A victims' hesitancy or unwillingness to participate in the criminal justice system–due to witness intimidation, dynamics of power and control, or feelings of love and loyalty toward the perpetrator–must be carefully examined in order understand how best to help victims and prosecute these cases.[2] Less experienced/untrained law enforcement officers and prosecutors may not recognize legitimate reasons for victim recantation, fail to investigate and prepare the case in anticipation of a possible recantation, or understand how these cases can proceed without victim testimony.

Like domestic violence, sexual assault involves uniquely vulnerable victims, and poses challenges for prosecutors and other professionals in the criminal justice system. How these crimes happen, who commits them, and who is victimized—are widely misunderstood by those untrained about perpetrator-victim dynamics and the neurobiology of trauma. Specialized training, meticulous case preparation, and compassionate and research-informed interactions with victims and witnesses are critical to successfully proceeding in these cases.

We know domestic violence and sexual violence incidences are severely underreported. With that in mind, Ripley County is a jurisdiction of approximately 30,000. In 2019, there were 90+ reports of domestic violence and less than 15 reports of adult sexual violence in Ripley County. There are many barriers to reporting these crimes, and I recognize that Ripley County is not immune to underreporting. The challenges domestic violence and sexual violence cases present are significant, but not insurmountable. We must work together to employ additional and new, evidence-based practices to tackle them. Below, I offer recommendations adapted from national resources addressing best prosecution practices because they mirror my own experiences in the field.

Recommendation 1: Enhanced Training for Law Enforcement Responding to Domestic Violence Cases

In domestic violence cases, prosecutors and law enforcement can employ strategies to enhance a victim's willingness to participate in the prosecution of their abusers, and even

the chance of prosecutorial success without victim participation. In the latter scenario, preparing and litigating forfeiture by wrongdoing motions[3], which can counter confrontation challenges in certain cases, is critical, and depends on evidence gathered by meticulous investigations, conducted by well-trained officers who understand the dynamic of domestic violence. Typical tactics supporting evidence based prosecutions include: conducting pretext phone calls (where appropriate), monitoring the defendant's phone calls from jail, reading any written communications to the victim, and working with medical and other experts to interpret and explain injury, lack of injury, common dynamics, and other important evidence. These investigations often reveal additional witnesses crucial to corroborating details of the crime when the victim is unwilling or unable to participate in the prosecution, and prioritize the documentation of information critical to overcoming hearsay or confrontation objections to the absent victim's out-of-court statements.[4]

By employing the principles of evidence-based prosecution, prosecutors are able to counter the challenges posed by gaps in the evidence, as well as legal challenges arising from a victim's lack of participation. Much of this corroborating evidence may also be relevant to admission of a victim's out-of-court statements by establishing that the defendant forfeited his right to confrontation. Thorough investigation and documentation[5], therefore, is critical in allowing prosecutors to anticipate—and prepare for—cases where the victim does not participate in prosecution.

Recommendation 2: Development of Specialized Prosecutors and Law Enforcement Responding to Domestic and Sexual Violence Cases

Specialized prosecution units promote the development of expertise, and provide access to focused training and collaboration opportunities with allied partners.[6] The research shows, however, that a specialized unit alone will not improve prosecution rates unless the prosecutors assigned to it are specially trained, aggressive, informed, and skillful trial attorneys, who measure success beyond conviction rates. Specialized investigative practices aid in uncovering relevant evidence and encourage victims to remain engaged throughout the process. Specialized trial expertise provides the necessary knowledge and skills to explain common gaps in evidence and counter deeply entrenched myths and assumptions about victim credibility—namely what trauma and victimization look like.

Experience, knowledge, and analytical skills are critical in identifying and correctly applying the criminal statutes, evidentiary and procedural rules, and case law relevant to the prosecution of sex crimes. Prosecutors must also be familiar with the current research related to: victim behavior, perpetration, medical/health issues, forensic science, and psychological/mental health issues. Moreover, specialized prosecutors must understand the common challenges that arise when investigating and prosecuting these crimes.

Offices can specialize by implementing hiring, assignment, and targeted training processes that identify and develop compassionate prosecutors with the skills necessary to succeed in prosecuting sexual and domestic violence. Prosecutors who have performed well in general crimes, crimes against persons, or violent crimes, who have the desire and disposition to develop the necessary expertise and to give these cases the attention they deserve, are possibly good candidates for specialization because of their expertise engaging with victims.

Recommendation 3: Commit to Trauma-Informed, Victim-Centered and Offender-Focused Sexual and Domestic Violence Prosecution.
Starting from a place of neutrality is critical, as it ensures trainings, practices, policies, and philosophies are trauma-informed, victim-centered, and offender-focused. A trauma-informed approach acknowledges trauma is an individual response to physically or emotionally harmful events, recognizes the offender is responsible for the victim's trauma, aids in identifying and interpreting of evidence of trauma, and assists juries in understanding its effects. Interaction with victims minimizes re-traumatization and maximizes their engagement with the criminal justice system.[7]

A victim-centered approach appreciates the central role victims play in the judicial process and demands law enforcement partners consider their needs throughout the process. An offender-focused approach recognizes that offenders purposefully and intentionally target victims whom they believe they can assault and impugn in order to avoid the consequences of their conduct. Importantly, it focuses on the offender's actions and intent and opposes defense tactics to deflect the focus on to the victim. These two approaches are not mutually exclusive, however, and prosecutors must weave the two together in order to ensure a trauma-informed prosecution.

In light of this, prosecutors should specialize in handling sex crimes, domestic violence, stalking, human trafficking, and/or child abuse cases, rather than carrying a mixed caseload of generalized crimes. This can enhance the assignment of trauma-informed practices and personnel to support victims through the criminal justice process.

Recommendation 4: Pretrial Motions, when possible, should be filed.
Pretrial motions enable us to keep out irrelevant and prejudicial information which open up the victim to attack on issues unrelated to their victimization. Such motions include those related to safety, rape shield, admissibility of hearsay and other evidence under federal or state rules. At the same time, prosecutors must file motions to introduce evidence pertaining to the offender's other acts, e.g., under FRE 404(b), or behaviors indicative of consciousness of guilt, and admissions, as well as sentencing enhancements for repeat offenses, gang activity, use of a firearm, or other factors.[8]

Recommendation 5: Engage in More Meaningful Multidisciplinary Collaboration
A comprehensive, successful response depends upon all system stakeholders–including medical forensic examiners and victim advocates. Strong collaboration among these professionals is essential; if one organization does not do its job well, prosecutions can be compromised.[9] Research shows that a system working collaboratively to provide a coordinated response encourages more victims to access services and participate in the process, better holds offenders accountable, and improves victim and community safety. Collaboration also enables allied professionals to share resources, educate one another, evaluate, refine their practices, adapt to emerging issues, and ensure the sustainability of their practices.[10] Prosecutors should identify and encourage collaboration with leading experts in these multidisciplinary fields to better understand victim experiences and develop deeper insight into sexual assault case evidence.[11] Some multidisciplinary partners not involved in the case may be qualified as experts to offer expert testimony on victim behavior and should be utilized whenever applicable and possible.

Engagement in Sexual Assault Response Teams (SARTs), represents an important way to "[e]nsure justice and create a more compassionate and streamlined response, [allowing] service providers [to] intervene in a way that speaks to the context of each victim's circumstance and respects the unique roles of the different professionals involved in responding to sexual assault."[12] Prosecutors should take a leadership role in the SART in their community and ensure *consistent* participation, preparation, and mentoring of staff assigned to the team.[13] They should also create a mechanism for receiving and responding to feedback from their community partners, sexual assault victims who have reported, and those who choose to remain anonymous or decided not to report.[14]

Recommendation 6: Recognize, Prevent, and Respond to Witness Intimidation.
Witness intimidation is a common issue that must be confronted at the outset of a case and throughout its prosecution. Without addressing it early on, witness intimidation can lead to destruction of a case, send a message to offenders that they control the criminal justice process, and cause additional trauma and injury to victims. Prosecutors should work with law enforcement and corrections to ensure an investigator immediately talks to the victim and witnesses so they understand what types of conduct constitute intimidation and how to safely report it. A prosecutor should, when possible, file charges, motions to revoke bond, and/or include the intimidating conduct in the prosecution of the underlying case.[15]

Recommendation 7: Obtain More Accurate Data on the Incidence of Sexual Violence to Determine the Rate of Victim Reporting to Law Enforcement and Percentage of Cases to Which Prosecutors are Responding.
Nationwide research suggests that many, if not most, incidents of sexual violence never result in criminal charges. By obtaining a clearer picture of sexual violence's scope in our communities, the reasons for nonreporting, and the rates of case attrition (the rate at which cases are "lost" or dropped), law enforcement and prosecutors can begin to assess the extent to which their own actions, as well as the actions of allied professionals in other agencies, are affecting these numbers.

Accurately calculating the prevalence of sexual assault in one's jurisdiction, as well as the rate and causes of attrition is a huge undertaking and could benefit from partnerships among allied professionals. Prosecutor's offices that have dedicated analysts incorporating and integrating data into its practice might be able to capture this number. However, prosecutors can also work with partners to obtain initial estimates for purposes of developing a very general, big-picture view of the extent and sources of attrition.

Recommendation 8: Ensure Unbiased and Well-Informed Standards for Charging and Prosecuting Sex Crimes
Inappropriate declinations tend to rest on two discrete, equally problematic practices: the initial—often inaccurate—impression of the case facts or victim, and the speculation or prediction about the likely outcome. Initial impressions that result in declination are often the product of premature judgments formed before all facts are known. Decisions to forgo full investigations sometimes flow from an intent to prioritize expenditure of finite resources for those crimes perceived as most likely to be substantiated and prosecuted.[16] However, improved investigations strengthen complex cases and improve the likelihood of a positive trial outcome. Results of recent research into untested sexual assault kits

should remind us of the consequences these decisions have for victims and communities, where failure to properly investigate and adequately communicate among allied professionals have resulted in perpetrators remaining free to possibly assault others.

Speculation about likelihood of conviction describes prosecutorial decision making based on what we believe a jury would do rather than based on what they should do. The "would" rather than "should" approach is also known as predictive analysis and "involves prosecutors in predicting the future decision-making of others… [and] if the persons who will make the ultimate decision at trial are unlikely to find the evidence sufficient, then the prosecutor… [will] decline prosecution on grounds of evidential insufficiency."[17] Collateral consequences put in motion from this approach includes law enforcement not referring cases for prosecution if they believe the prosecutor is unlikely to charge, based on the prosecutor's professed belief that juries will not convict on a given set of facts. Predictive analysis is at odds with the proper basis for prosecutorial discretion because it abdicates the critical decision-making responsibility to a less than fully informed, hypothetical jury. Prosecutorial decision making must focus on whether a factfinder, provided with the education (e.g., through expert testimony) and reviewing all available and admissible evidence, should render a guilty verdict. This method alone is in line with our duty as prosecutors to ensure the guilty do not escape and the innocent do not suffer as well as to use all legitimate means to bring about justice.[18]

In light of this, prosecutors should identify practices that result in little or no investigation, leading to cases that are inappropriately or prematurely closed without charges or referral to the prosecutor. Specialized prosecutors should review ***all*** police reports to determine which types of cases and victims are being passed over and why.

Recommendation 9: Develop a Comprehensive and Measurable Definition of Success in Sexual Violence Cases

The process of prosecuting a sexual assault case is arguably as important as its outcome. Even if a case results in a resolution that falls short of the charges or sentence pursued by the prosecutor, the implementation of best practices throughout the life of the case—from initial evaluation and charging through resolution—can generate a high quality of procedural justice for the victim and the public. A comprehensive definition of case success should thus account for prosecution efforts to bring about justice. There are multiple measures to consider, including: case resolution, which takes into account case complexity; the implementation of best prosecution practices throughout case processing; and the victims' experiences with their case and the quality of treatment they received.[19]

Recommendation 10: Enhance Training on Prosecuting Alcohol-Facilitated Sexual Assault

Alcohol is the most common weapon used to facilitate sexual assault. Offenders use alcohol because it renders victims vulnerable, affects memory, and impairs judgment and physical ability. These cases present unique complexities in identifying corroborating evidence, interviewing victims, explaining basic toxicology, differentiating between "passouts" and "blackouts," and understanding the effect of societal attitudes about alcohol on determinations of victim credibility.[20]

[1] *See* WOMEN PROSECUTORS SECTION, NAT'L DIST. ATTORNEYS ASS'N, NATIONAL DOMESTIC VIOLENCE PROSECUTION BEST PRACTICES GUIDE (2017), available at http://ndaa.org/wp-content/uploads/NDAA-DV-White-Paper-FINAL-revised-July-17-2017-1.pdf.

[2] *See* Jeffrey Sonnis et al., *Risk and Protective Factors for Recurrent Intimate Partner Violence in a Cohort of Low-Income Inner-City Women*, 23 J. FAM. VIOLENCE 529–538 (2008), *available at* https://doi.org/10.1007/s10896-008-9158-7; Emma Birdsey et al, *Reporting Violence to Police: A survey of victims attending domestic violence services*, 91 Bureau of Crime Stat. & Res. (2013), *available at* https://www.women.nsw.gov.au/__data/assets/pdf_file/0004/280912/Reporting_Violence_to_the_Police_-_BOCSAR_survey.pdf; and Amy E. Bonomi et al., *"Meet me at the hill where we used to park": Interpersonal Processes Associated with Victim Recantation*, 73 SOC. SCI. & MED. 1054 (2011), *available at* https://www.familyjusticecenter.org/wp-content/uploads/2018/09/Meet-Me-at-the-Hill-Where-We-Used-to-Park-Interpersonal-Processes-Associated-with-Victim-Recantation.pdf.

[3] *See* TERESA M. GARVEY, LEGAL JIU-JITSU FOR PROSECUTORS IN INTIMATE PARTNER VIOLENCE CASES: FORFEITURE BY WRONGDOING, 17 STRATEGIES (Dec. 2018), *available at* https://aequitasresource.org/wp-content/uploads/2018/12/Legal-Jiu-Jitsu-for-Prosecutors-in-IPV-Cases-Forfeiture-by-Wrongdoing-2.pdf (for a discussion of the use of forfeiture by wrongdoing).

[4] *See, e.g.*, Michigan v. Bryant, 131 S.Ct. 1143 (2011) (for discussion of ongoing emergency); *see also*, Herb Tanner & John Wilkinson, *Supreme Court Clarifies the "Ongoing Emergency" in Michigan v. Bryant*, 9 STRATEGIES IN BRIEF (Dec. 2011), *available at* http://www.aequitasresource.org/Supreme_Court_Clarifies_Ongoing_Emergency_in_Michigan_v_Bryant_Issue_9.pdf.

[5] Jennifer Gentile Long & Teresa Garvey, *No Victim? Don't Give Up*, 7 STRATEGIES (Nov. 2012), *available at* https://aequitasresource.org/wp-content/uploads/2018/09/S_Issue_7_No_Victim-Dont_Give_Up.pdf.

[6] Dawn Beichner & Cassia Spohn, *Prosecutorial Charging Decisions in Sexual Assault Cases: Examining the Impact of a Specialized Prosecution Unit*, 16 CRIM. JUST. POL'Y REV. 461 (2005).

[7] *See* VIKTORIA KRISTIANSSON, AEQUITAS, CAMPUS-RELATED CRIMES OF SEXUAL VIOLENCE: TRIAL PACKET FOR PENNSYLVANIA JUDGES 18 (2016) (citing Rebecca Campbell, et al., *Responding to Sexual Assault Victims' Medical and Emotional Needs: A National Study of the Services Provided by SANE Programs*, 29(5) RES. IN NURSING & HEALTH 384 (2006)).

[8] For additional information on filing pretrial motions, *see* AEQUITAS, EVIDENCE OF OTHER "BAD ACTS": INTIMATE PARTNER VIOLENCE, SEXUAL VIOLENCE, STALKING, AND HUMAN TRAFFICKING PROSECUTIONS, 31 STRATEGIES (May 2017) *available at* https://aequitasresource.org/wp-content/uploads/2018/09/Evidence-of-Other-Bad-Acts-In-Intimate-Partner-Violence-Sexual-Violence-Stalking-and-Human-Trafficking-Prosecutions.pdf.

[9] *See* AEQUITAS, JMI, AND THE URBAN INSTITUTE, MODEL RESPONSE TO SEXUAL VIOLENCE FOR PROSECUTORS (RSVP MODEL) VOLUME I: INVITATION TO LEAD 27, *available at* https://aequitasresource.org/wp-content/uploads/2020/01/RSVP-Vol.-I-1.8.20.pdf.

[10] *See id.* at 9; *see generally* AEQUITAS, JMI, AND THE URBAN INSTITUTE, MODEL RESPONSE TO SEXUAL VIOLENCE FOR PROSECUTORS (RSVP MODEL) VOLUME I, II AND III, *available at* https://aequitasresource.org/wp-content/uploads/2020/01/RSVP-Vol.-I-1.8.20.pdf.

[11] RSVP citing *See* Rebecca Campbell, et al., *Adolescent Sexual Assault Victims and the Legal System: Building Community Relationships to Improve Prosecution Rates*, 50(1-2) AM. J. COMMUNITY PSYCHOL. 141-54 (2011); Rebecca Campbell et al., *Prosecution of Adult Sexual Assault Cases: A Longitudinal Analysis of the Impact of a Sexual Assault Nurse Examiner Program*, 18(2) VIOLENCE AGAINST WOMEN 223-44 (2012); and AEQUITAS, LITERATURE REVIEW: SEXUAL ASSAULT JUSTICE INITIATIVE (2017).

[12] RSVP citing *What is a SART?* SART TOOLKIT, https://ovc.ncjrs.gov/sartkit/about/about-sart.html (last visited Mar. 4, 2017). Please note that convening a sexual assault task force to discuss the potential formation of a SART/MDT is an initial step – it takes some time to discuss and agree upon MOUs and confidentiality agreements.

[13] *See* AEQUITAS, JMI, AND THE URBAN INSTITUTE, MODEL RESPONSE TO SEXUAL VIOLENCE FOR PROSECUTORS (RSVP MODEL) VOLUME I: INVITATION TO LEAD 27, *available at* https://aequitasresource.org/wp-content/uploads/2020/01/RSVP-Vol.-I-1.8.20.pdf.

[14] Feedback from victims who have opted out of the criminal justice system can be obtained via a hotline (perhaps one established within the crime victim rights and compensation office), victim's rights organization, civil attorneys, or community-based service provider, all of which interact with survivors in the aftermath of an assault. RSVP Volume II, Chapter 9.

[15]AEquitas led 2 special initiatives, "Combatting Witness Intimidation" and "Improving the Justice System Response to Witness Intimidation," both of which worked with pilot sites to enhance strategies to prevent, identify, and respond to, witness intimidation. For more information, visit https://aequitasresource.org/initiatives/ and visit Past Initiatives; *See also*, *Special Initiatives: Improving the Justice System Response to Witness Intimidation",* AEQUITAS: THE PROSECUTORS' RESOURCE ON VIOLENCE AGAINST WOMEN, http://aequitasresource.org/special-initiatives.cfm. IWI was a field-initiated project funded by the U.S. Department of Justice, Bureau of Justice Assistance (BJA) award number 2010-MU-BX-K079;

[16] Training both law enforcement and prosecutors in core competencies (identified in Appendix B of the RSVP Appendices) and fostering multidisciplinary collaboration can help with appropriate decision-making. The RSVP Appendices can be found at https://aequitasresource.org/wp-content/uploads/2020/01/RSVP-Appendices-1.9.20.pdf.

[17] Michelle Madden Dempsey, *Prosecuting Violence Against Women: Toward a "Merits-Based" Approach to Evidential Sufficiency*, VILLANOVA UNIVERSITY SCHOOL OF LAW (2016).

[18] *Berger v. United States*, 295 US 78, 88; 79 L.Ed.1314 (1935).

[19] *See* AEQUITAS, JMI, AND THE URBAN INSTITUTE, MODEL RESPONSE TO SEXUAL VIOLENCE FOR PROSECUTORS (RSVP MODEL) VOLUME I: INVITATION TO LEAD; VOLUME II: MEASURING THE RESPONSE & APPENDICES. The Model Response to Sexual Violence for Prosecutors (RSVP) includes a collection of office- and case-level promising practices, identified through research and the experience of both AEquitas staff and partnered prosecutors. It also includes a comprehensive tool for tracking measuring and continuously enhancing the prosecution of sexual violence. For more information visit https://aequitasresource.org/resources/ .

[20] For additional information on alcohol-facilitated sexual assault, *see* Teresa Scalzo, Prosecuting Alcohol-Facilitated Sexual Assault, NAT'L DISTRICT ATT'Y ASS'N. (2007), *available at* http://biblioteca.cejamericas.org/bitstream/handle/2015/3185/pub_prosecuting_alcohol_facilitated_sexual_assault.pdf?sequence=1&isAllowed=y, ; *See also* RSVP MODEL, Appendix G. *Stages of Acute Alcohol Influence/Intoxication*. For additional information visit https://aequitasresource.org/resources/.

Chief Robert Hawkins

Muscogee (Creek) Nation Lighthorse Police Department

Robert Hawkins is the Chief of Police for the Muscogee (Creek) Nation Lighthorse Police Department. The Muscogee (Creek) Nation is the fourth largest tribe in the United States, and is comprised of 11 counties, approximately, 7,200 square miles, located in Northeast Oklahoma.

Mr. Hawkins has been in law enforcement for 23 years, beginning his career in 1997 as a Reserve Police Officer for the City of Altus, Oklahoma, which is his hometown. In 2000, he began as a police officer for the City of Hollis, Oklahoma, and was appointed Chief of Police in 2005. Mr. Hawkins served as Hollis Chief of Police until 2011 when he relocated to the Tulsa metropolitan area and joined the Muscogee (Creek) Nation Lighthorse Police Department as a patrol officer. In 2013, he was reassigned to the Investigations Division and in December, 2015, was appointed Lighthorse Chief of Police, officially taking charge of the department on January 1, 2016. The Lighthorse Police Department is comprised of 66 employees; 55 sworn officers, 7 Communications officers and 4 Administrative support staff.

The following was taken from the written transcript of Chief Robert Hawkins' oral testimony.

My name is Robert Hawkins, I am the Chief of Police for the Muscogee Creek Nation Lighthorse Tribal Police Department in Oklahoma. I have 23 years law enforcement experience -- 9 as a criminal investigator, and 11 as Chief of Police. I have served on the state and tribal jurisdiction side.

Today I will be discussing how tribal law enforcement handles cases of domestic violence and sexual assault. From communicating with advocates on the tribal and stateside, working with other local, state, and federal law enforcement agencies, how evidence is processed, and what law enforcement can do to improve the dealings with these crimes.

As we know, when law enforcement responds to a domestic violence and/or a sexual assault, all avenues of the incident are put in play -- such as the well-being of the victim, identity and/or number of suspects, location of the crime, and the safety of the officers responding to the call.

Investigating domestic violence and sexual assault cases on tribal land can be and is difficult at times. This is due to the issues we have with jurisdiction. The Muskogee Creek Nation tribal boundaries span 11 counties, approximately 7200 square miles. The city of Tulsa is the largest area within our jurisdiction. We have a total population in the metropolitan area of Tulsa of about 1.1 million, so things can get rather complex when it comes to having to figure out our jurisdictional bounds.

Our tribal law enforcement jurisdiction consists of restricted and trust lands and properties held by the tribe. So to determine where the crime occurs plays into what law enforcement agency, whether it's tribal, state, or federal, has jurisdiction to prosecute the suspects in the crime. What helps my agency with the issues of jurisdiction is that we hold a cross-deputization with most - all of the municipal and county law enforcement agencies within the Creek nation boundaries.

That is about 42 law enforcement agencies that we are cross-commissioned with. Having these cross-deputizations enables my agency, as well as the state-side jurisdiction agencies, to deal with any crime that has occurred on tribal and non-tribal lands and properties. My department has a very good working relationship with all these agencies, which makes for a safer environment for the officers of all the agencies involved, as well as the victims of any crime.

Another factor that determines jurisdiction in dealing with these cases is who is involved in the crime. Jurisdiction is determined by whether the crime is committed by a native on non-native, native on native, non-native on native, or non-native on non-native.

The Violence Against Women Act allows a tribal agency to prosecute a non-native perpetrator who committed a domestic violence and/or sexual assault on a native female victim. Last year the Muscogee Creek Nation was the first tribe to successfully prosecute a non-native suspect in tribal court on domestic assault against a female tribal citizen.

So as you can see, investigating these crimes committed in Indian Country, is rather complex. When it comes to domestic violence and sexual assault cases, the Creek Nation takes them very seriously. And I can speak for many of the other tribes in the state of Oklahoma that deal with the same cases. Just speaking to the other four large tribes: The Cherokee, Choctaw, Chickasaw, and Seminole nations, in reference to domestic violence and sexual assault cases, our agencys' calls of this nature are approximately 30%, which is significant.

So what's important for law enforcement on the tribal side is to have good collaboration with local, state, and federal agencies, but most important with the advocates from their family violence and sexual assault programs. When my officers respond to one of these calls, once we secure the scene and the victim, and if medical personnel are needed and are called, we contact our advocates with the tribe's family violence and sexual assault department. Keep in mind this just isn't for our native victims. This is for all victims of these crimes.

Of course, if the crime occurs off tribal land, the jurisdictional agency, as well as the Oklahoma Department of Human Services, would be contacted and respond to the crime scene. At which time they would take control of the incident.

However, my agency responds to all calls outside of jurisdiction when it comes to our citizens. While on scene, my officers and the advocates do a lethality assessment on the victim. The victim is assessed, then taken to be medically checked if need be. Officers and advocates make sure the victim is safe, whether it's in the victim's home or taking them to a shelter. If a sexual assault has occurred, then the victim is advised of what needs to be done, and if consent is given, the victim is taken to our tribal medical center, where a sexual assault exam is conducted by the tribe's certified SANE nurse.

At that point, the investigation gets into high gear. In the course of the investigation, my Investigations Division is called to the scene immediately after the call is received. They process the scene thoroughly, precisely, and completely. My agency follows protocols when handling evidence. Whatever it is, it's collected and stored. Evidence can be stored as long as possible while the investigation is ongoing. There is a precise chain of custody, and complete and thorough documentation of all evidence.

All evidence is collected and is stored in our evidence room until it can be sent to the lab for analysis. Sexual assault evidence is sent to the lab as soon as possible. Our practice is to have it to the lab within 24 hours - that's the rape kit and everything that goes along with the sexual assault.

I have a very good Investigations Division, and they communicate well with outside jurisdictional agencies. Any evidence or information gathered at a scene, whether a domestic violence or sexual assault case, where the jurisdiction lies with the local or state agency, a report is generated. In an agency assist, all items and documentation are turned over to that agency. And for sexual assault cases that fall under the Federal Major Crimes Act, our investigators will contact the FBI and relay information to them as required by federal law.

Most crimes for which we contact the FBI have occurred on our tribal land, restricted or trust properties. The FBI will send their sex crimes agent to meet with my investigators and conduct their protocol investigation of the incident. There are typically no issues with my Investigations Division when it comes to the collection and processing of evidence and working and collaborating with other agencies.

To date, we have a 92% solve rate on sexual assault cases and a 90% solve rate on domestic violence cases. This is all in part of the working relationship we have with the advocates and other law enforcement agencies.

As for what law enforcement could do better when handling these types of calls:

1) Advanced training for law enforcement officers is essential. This helps them become better educated on what they can do and how to handle domestic violence and sexual assault cases.

2) Ensure the victims receive legal protection from harm, meaning whatever needs to be done to help the victims to obtain protective orders and/or a safe haven. It's important that the victims know they are safe and we're going to protect them.

3) Increase victim, community, and officer safety. When we have an incident where domestic violence or a sexual assault has occurred, our victim of course is looked upon by our officers. We issue what we call watch orders on residences of the victims, increasing patrols throughout our communities, and in doing so with more numbers of officers. By being seen, citizens feel more safe.

4) Encourage victims to report the crimes when they happen. Too many times officers have arrived at a scene of a domestic or sexual assault and were told that it wasn't the first time the incident has occurred. Victims should be urged to report the crime each time so that law enforcement can apprehend the perpetrator and the courts can prosecute to the full extent of the law.

5) Encourage victims and witnesses to cooperate with officers and investigators so that a solid case can be made against the perpetrator.

6) All offenders need to be held accountable for their actions. If you commit the crime, you do the time, as the saying states.

7) Law enforcement needs to strengthen the trust between their agency and the communities they serve. Community outreach is a great way to provide information about what resources law enforcement can provide to a victim of domestic violence or sexual assault. Being involved in the community will make the community, the public, trust officers and make citizens feel safe.

It's complex when it comes to dealing with any crime on tribal lands, because of jurisdictional issues and whether the perpetrator and victim are native or non-native. I thank you all for giving me this opportunity to speak today. Thank you.

Wednesday, April 15, 2020

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.

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

Good afternoon Chairman Keith, Vice Chair Sullivan, commissioners and distinguished guests. Thank you for inviting me to testify today.

My name is Darrin Jones, I am the Executive Assistant Director for the Science and Technology Branch at the FBI. It is from within this branch that the FBI effectuates federal court orders for the interception of communications and assists our field offices in accessing a wide range of digital evidence. I've had a front row seat to witness the steady erosion of Law Enforcement's ability to access electronic evidence and conduct court authorized electronic surveillance.

Over the last decade, a number of major US tech companies have chosen to independently design, develop, and then implement certain forms of technology, in this case increasingly complex, user-controlled encryption, ostensibly, in ways that no one other than the users can readily or timely access the contents of communications or other stored data. As is well known, this results in the creation of "lawless spaces" on the internet where law enforcement, even when armed with a Constitutionally-sound search warrant or wiretap order, are incapable of readily penetrating. These "lawless spaces" represent an ever-expanding universe of illegal and illicit activity, which threatens the lives and safety of our children, our economy, our national security, and even our elections.

In addition to my position at the FBI, I also currently serve as co-chair of the Commission's Technology Working Group. On behalf of that working group I would share the following recommendation:

> **Federal legislation must be enacted to compel major technology companies to design for themselves strong encryption regimes for their products and services that protect privacy but that permit lawful access pursuant to the due process of law.**

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

That language may sound familiar to many of you. The working group decided to mirror the language adopted by resolution in December 2019 by more than 30,000 IACP members representing over 160 countries.

For more than 200 years our Constitution, the Fourth Amendment, and our courts have balanced our privacy and the need for law enforcement to have access to the evidence society need to stop criminals, pursue justice for victims, and protect its citizens. Why should it be different in the digital world? We now find ourselves in a place where not the courts, but individual companies are deciding what's of greatest importance for all of us. Put another way, we're allowing technology to dictate our national core values rather than ensuring our national core values drive how we implement technology.

It has now been 131 days since a foreign terrorist in Pensacola, Florida, murdered in cold blood, three US service members on a US military base. Then, before being killed in a shootout with law enforcement, the terrorist took the time to put a bullet in his phone in a clear attempt to destroy it and all evidence it contained. We are still trying to access that phone. That's what I mean when I say we have a "lawful access" problem.

In a recent Gang Task Force case, source reporting and traditional telephony intercepts indicated that the main subject, suspected of ordering the homicide of another drug dealer, was using Facetime to discuss and coordinate criminal activity with his co-conspirators. Indeed, he frequently directed them to use FaceTime instead of traditional cellular telephones because FaceTime, a product of Apple uses, end-to-end encryption. Investigators, realizing they would not recover the content of FaceTime communications, did not pursue legal process. Post-arrest statements by the subjects confirmed they were well aware that those **not** arrested were only those co-conspirators exclusively using encrypted communications. That's what I mean when I say Law Enforcement has a "lawful access" problem.

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

Similarly, a recent OCDETF (Organized Crime Drug Enforcement Task Force) case indicated multiple subjects responsible for illicitly transporting large quantities of heroin, methamphetamine, cocaine and marijuana from the southern border to the Great Lakes region for further distribution regularly used encrypted apps to evade law enforcement detection. Senior members of the drug trafficking organization routinely instructed underlings to use WhatsApp, Telegram or Snapchat. Communications that would go unanswered on traditional cellular telephones were immediately accepted and responded to using encrypted Apps. Due to the inability to obtain content, OCDETF investigators did not pursue a Title III order. That's what I mean when I say we have a "lawful access" problem.

As most of you are aware, Mr. Zuckerberg has announced that he intends to encrypt FB Messenger soon. What that means is, one man has independently decided to implement technology, in this case end-to-end encryption, in such a way that even if a judge issues a warrant, no one, including law enforcement, can access those messages. In 2019 Facebook's platforms, primarily Facebook Messenger, sent over 15M tips to the National Center for Missing and Exploited Children. NCMEC immediately forwarded those tips to state and local law enforcement agencies across the country. They took them to judges, who issued warrants, which allowed those agencies to rescue thousands of kids. One man, one company is independently deciding whether or not that should continue.

The ubiquity of end-to-end encryption and other user-only access encryption products and applications causes them to be encountered nearly daily by state and local police departments. The impact of this challenge not only means an increase in unsolvable crimes and a denial of justice for victims, but also threatens to dramatically alter the nation's dual-sovereign federal system of law enforcement. Let me tell you how, because this may not be intuitive. When local police departments are without resources to timely and cost-effectively gain lawful access to critical criminal evidence that has been encrypted, they will necessarily have to turn to larger federal agencies such as the FBI for assistance. Under such a paradigm, the foreseeable result

may be that a federal agency may reluctantly but practicably find itself in the position of effectively dictating which state and local crimes are investigated and prosecuted regardless of the priorities of state and local officials. State and local agencies must maintain lawful access to electronic evidence in order to retain their basic jurisdictional sovereignty and to ensure that enforcement of local crimes is controlled at the local level.

In response, a number of major tech companies and academics have publicly proffered a solution to the lawful access challenge which is arguably as inappropriate as it is disingenuous: namely, that law enforcement should develop better hacking skills to keep pace with industry products, even though these same companies freely admit that they would quickly work to block any exploit used by law enforcement to gain access in execution of a court order. The prospect of police departments, which are already confronting major traditional crime-fighting personnel and resource challenges, entering into what would, in essence, be a cryptologic arms race with Apple or Google is not only ludicrous, but it confirms the existence of an industry mindset which believes that it controls this public policy debate in place of democratically-elected governments.

The tech companies would have you believe that it's impossible to allow lawful access while maintaining strong cyber security. In response, Bill Gates, founder of Microsoft, has said, "[T]he companies need to be careful that they're not ... advocating things that would prevent government from being able to, under appropriate review, perform the type of functions that we've come to count on." When asked if he was referring to iPhone unlocking, Gates suggested: "There's no question of ability; it's the question of willingness." Butler Lampson—a winner of the Turing Award, the Nobel Prize of computer science—calls the approach "completely reasonable … The idea that there's no way to engineer a secure way of access is ridiculous."

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

I feel like I need to add that I am always personally stunned when I hear companies talking about law enforcement trying to build a "back door." We're not trying to build a "back door," to anything – we're asking companies to be able to open the door when law enforcement has a lawful court-authorized search warrant. What they're trying to do is block the door – build the door and barricade it – and prevent it from being opened by law enforcement, for any reason. They seem to be okay with using encryption to prevent law enforcement from opening the door and accessing the house whether or not there is a spy hiding behind the door, a terrorist behind the door who killed our sailors on a military base in our own country, an MS-13 member preparing to kill again, or a kidnapped child behind the door who needs to be rescued. They're openly telling us they're going to bar this door and make it impossible to enter with a warrant. I have to tell you, I am stunned when I hear this, each time, because these are the exact same companies who are simultaneously mining customers' data for information and even selling it to third party companies. And they say it's okay.

The impact and magnitude of the Lawful Access crisis in the United States has grown to a point where the public safety trade-off to the citizens of this country can and should no longer be made privately and independently in the corporate boardrooms of tech companies. It must, instead, be returned to the halls of the people's democratically elected and publicly accountable representatives.

Ladies and gentlemen let me be very clear. The FBI supports the use of strong encryption. It's critical to securing our infrastructure and our online privacy. But there are already strong forms of encryption used daily in the US in the regulated financial and securities sectors, which secure information yet provide for appropriate access. We firmly believe that strong encryption models can be implemented by these companies in a way that is in accord with long-accepted Constitutional theories of privacy and civil liberties, continues to support robust cyber security, and provides for court-ordered lawful access.

Darrin Jones, FBI; President's Commission on Law Enforcement and the Administration of Justice; Crime Reduction Hearing, April 15, 2020.

I would reiterate the Technology Working Group's recommendation: **Federal legislation must be enacted to compel major technology companies to design for themselves strong encryption regimes for their products and services that protect privacy but that permit lawful access pursuant to the due process of law.**

Thank you for your time, and I look forward to your questions.

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.

---

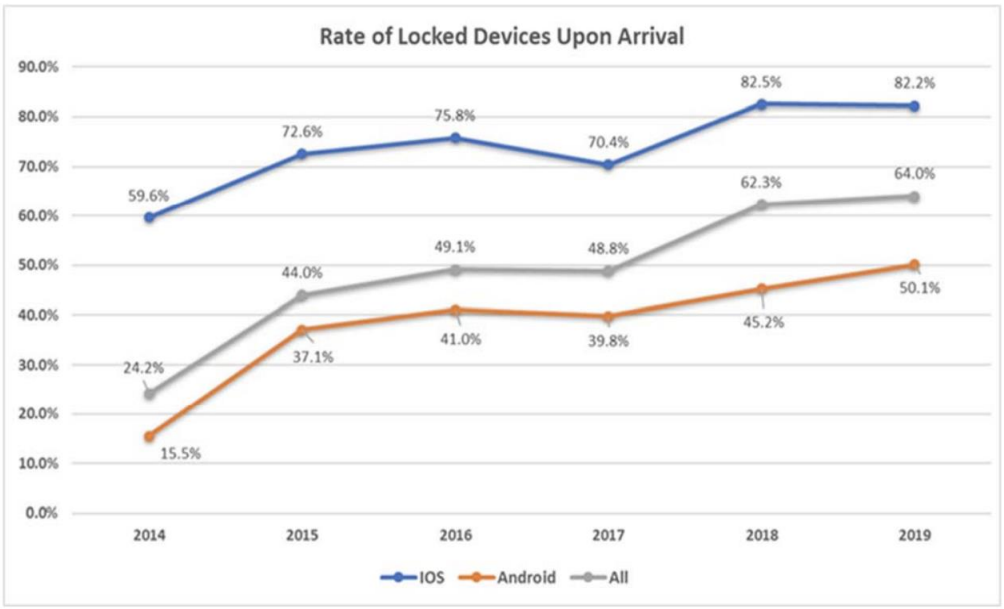
[6] Bruce Sewell, Senior Vice President and General Counsel for Apple, Inc., Responses to Questions for the Record, "The Encryption Tightrope: Balancing Americans' Security and Privacy," at p. 2. Question 6(b)(1). U.S. House Committee on the Judiciary, 1 March 2016. Was the technology you possessed to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

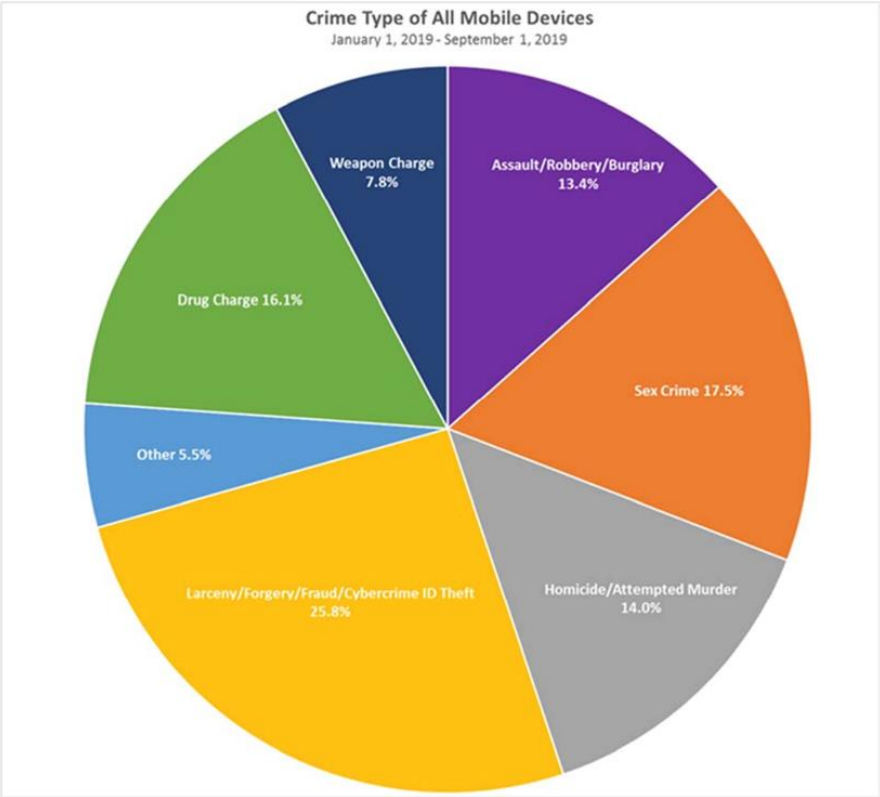
II. A GROWING PROBLEM WITH RAMIFICATIONS FOR OUR PUBLIC SAFETY AND ENTIRE SYSTEM OF JUSTICE

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.

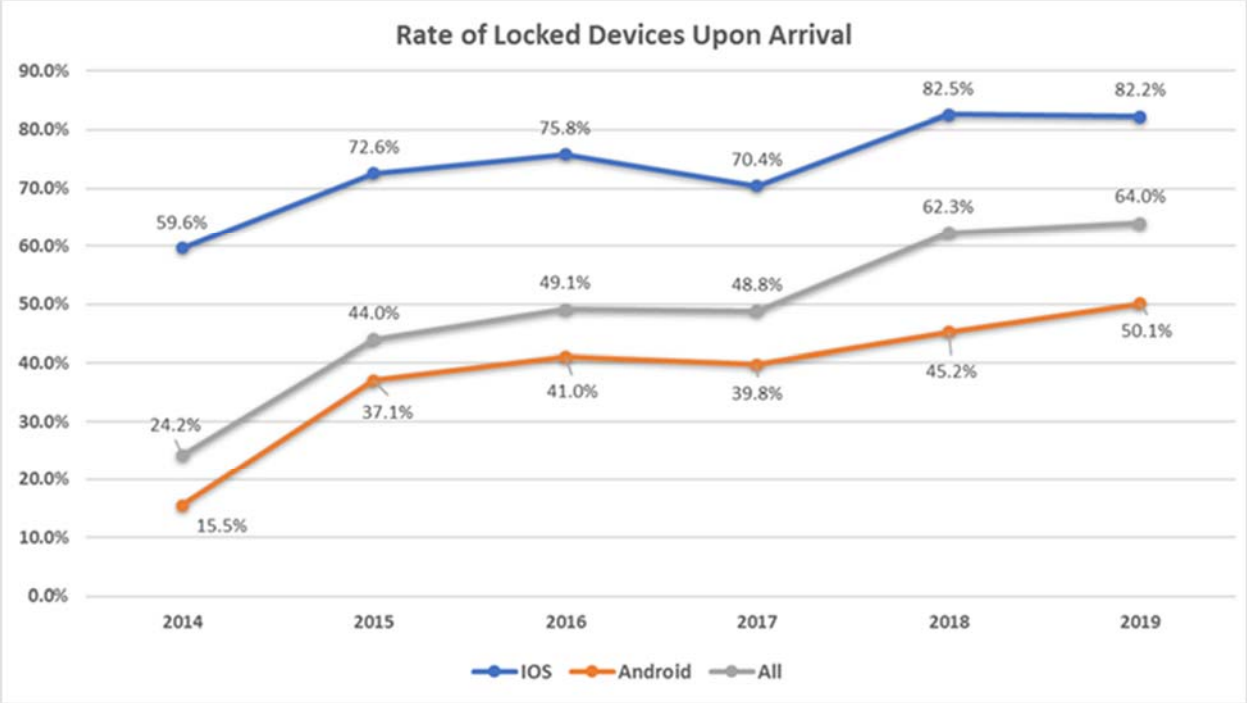
[7] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2017 Report*, Nov. 2018, *available at* https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf.

[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]

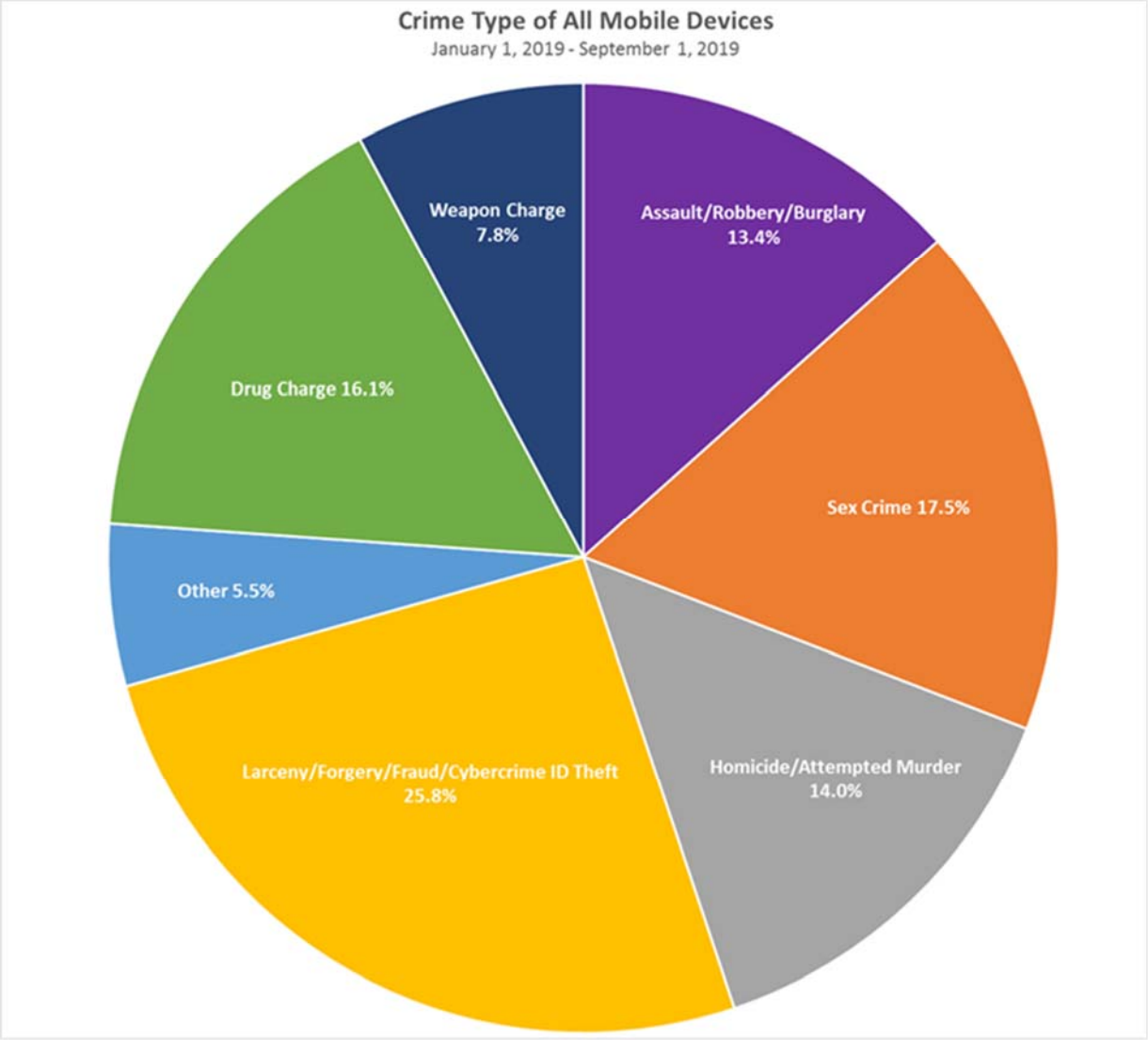
For our office and others, the number of encrypted devices containing important evidence remains high, with the trend of inaccessibility increasing each year. As the below chart indicates, the percentage of encrypted Apple devices arriving at our office has increased significantly over the past five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

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.

Thursday, April 16, 2020

Thomas G. Ruocco

Chief Criminal Investigations, Texas Department of Public Safety

Mr. Ruocco is Chief of the Criminal Investigations Division at the Texas Department of Public Safety. He oversees 832 employees statewide that conduct criminal enterprise investigations targeting those organized criminal groups that constitute the greatest threat to Texas. This includes programs focused on drug trafficking, human trafficking, gang activity and other specialized investigations such as fraud, cargo theft, human smuggling, vehicle theft and illegal gambling. CID works closely with local, state, and federal agencies to identify and arrest high threat criminals such as sex offenders and other violent fugitives. CID also provides technical investigative support both within the Department and to other law enforcement agencies.

Mr. Ruocco is a member of the International Association of the Chiefs of Police, where he serves as the chairperson of the Police Investigative Operations Committee; Association of State Criminal Investigative Agencies, where he served as chairperson of the Human Trafficking Committee; Criminal Intelligence Coordination Council, where he serves as the vice chairperson; National Domestic Communications Assistance Center, where he serves on the executive advisory board; and the National Association of Missing and Exploited Children, where he serves on the advisory board.

Mr. Ruocco is the former FBI Assistant Special Agent in Charge of the San Antonio Division, Austin Resident Agency. In this capacity, his duties included management and oversight of the Austin Resident Agency, Waco Resident Agency, and the Counterterrorism Program.

He is a native of New York and a graduate of St. John's University in Queens, New York, where he earned a Bachelor of Science Degree in Criminal Justice in 1980.

Mr. Ruocco began his career with the FBI at New York in a support capacity in September 1979. In September 1984 he was appointed as a Special Agent and served in the Atlanta, Georgia, Field Division and Brooklyn/Queens Metropolitan Resident Agency of the New York Field Division.

In May 1995 Mr. Ruocco was transferred to the San Antonio Field Office where he served as a field supervisor for a Violent Crimes squad, two White Collar Crime squads, and the Joint Terrorism Task Force. During this time, he served as the Program Coordinator for the Violent Crimes and Major Offenders Program, White Collar Crime Program and the Counterterrorism Program, and formulated the establishment of a Public Corruption squad.

In April 2003 Mr. Ruocco was assigned to FBI Headquarters in Washington, D.C., where he served over two years with the Office of Intelligence and the Inspection Division.

In January 2006 Mr. Ruocco was named the Assistant Special Agent in Charge of the San Antonio Division, Austin Resident Agency.

In July 2008 Mr. Ruocco retired from the FBI.

In February 2009 Mr. Ruocco began his employment with the Texas Department of Public Safety, when he was appointed chief of the Criminal Law Enforcement Division.

Thomas Ruocco
Division Chief – Criminal Investigations Division
Texas Department of Public Safety
Austin, Texas

Reduction of Crime Hearing: Strategies and Practices for Law Enforcement and Technology Use in Crime Reduction.

April 16, 2020

I would like to thank the Commission for affording me the opportunity to speak today. My name is Thomas Ruocco and I am the Chief of the Texas Department of Public Safety's Criminal Investigations Division. I am also the Co-Chair of the US Department of Justice's Technology Working Group, and my testimony will include some of the work and recommendations of that working group.

My division has more than 800 employees and conducts statewide investigations against criminal organizations that constitute the greatest threat to Texas. This includes investigations focused on drug trafficking, human trafficking, illegal gang activity, and other specialized investigations, such as fraud, cargo theft, human smuggling, vehicle theft, and illegal gambling. Our efforts are facilitated by the use of sophisticated technology and software-driven analytics to identify criminals and criminal activity. However, the technological ecosystem is rapidly evolving, and the expansion of communications technology makes collecting evidence much more complex than ever before. To succeed, law enforcement executives need to understand the complexities of this new digital environment when considering a multitude of factors, including:

- What new technologies to adopt and implement;
- How to utilize new data sources, including the aggregation and sophisticated analysis of existing data sources;
- What policy changes may need to be adopted; and
- How to work with both local communities and policy makers to ensure they fully understand the challenges and concerns each of these issues pose.

In addition, it is important that law enforcement agencies realize that the collection, analysis, utilization, and preservation of digital evidence must be managed under the same standards as other types of evidence. Therefore, law enforcement agencies need to adapt to manage the appropriate handling and use of digital evidence available from a multitude of resources.

After a review and discussion of these issues with the Technology Working Group, I have formulated two recommendations regarding how law enforcement should respond to the changing technological environment.

Recommendation #1

The first recommendation is for law enforcement agencies to employ a consistent and comprehensive framework when considering the adoption and implementation of new technologies.

Such a framework should be general enough to be applicable across a broad range of technologies, yet specific enough to ensure that agencies consider, at a minimum, the predictable significant costs and risks associated with a particular technology. Not all parts of the framework may be needed to address each technology, but the framework must be refreshed from time to time to accommodate new risks from emerging technologies.

Under this framework, agencies would first review the nature of a new technology to determine whether or not to adopt it; and then, secondly, determine how that technology would be prudently implemented within their organization. The transition point between these two phases will differ depending on the particular technology being studied. In addition, there will likely be information discovered during the adoption review phase that will drive and enhance elements of the implementation phase.

Framework questions asked during the adoption consideration phase may include:

- What are the initial and recurring costs associated with the technology?
- What are the legal or policy implications?
- What might be the public's reaction? and,
- To what additional risks might the agency be exposed should they choose to adopt the new technology?

Once an agency determines a particular technology should be adopted, the framework questions will naturally narrow and become more specific. For instance, framework questions asked during the implementation phase may include:

- How will the officers' work routines change as a result of the use of the new technology?
- What training is appropriate and how often must it be conducted? and,
- How will the use of the new technology be audited to ensure sensitive data is protected and the public confidence is maintained?

Recommendation #2

The second recommendation is for law enforcement agencies to employ a consistent and comprehensive framework when considering the creation or use of new data sets.

Some data sets may originate exclusively within an agency, such as officer productivity data or crime statistics, while other data sets may be obtained from sources outside an agency, such as commercial advertising data showing anticipated pedestrian flows for a given area or event. New

data sets can also be an amalgamation of both internal and external data, such as combining officer work schedules with actuarial data to better manage the risk of automobile or physical accidents.

Even in the case of well-defined, discreet data sets, it may be difficult for agencies to predict the full extent of consequences and benefits that may be associated with a new data set. New and much more sophisticated data aggregation and analysis techniques, such as Artificial Intelligence, may imbue new attributes or value to data not anticipated when it was first collected or obtained. A particularly poignant example is the Golden State Killer Case, in which forensic genealogy data that was originally collected to trace people's ancestry was effectively leveraged by law enforcement to identify a suspect in a cold case.

Framework questions associated with the creation or use of new data sets will flow along similar lines as those seen in dealing with new technologies. However, more care may be needed in setting up processes and putting in place safeguards to ensure agencies return to the framework when new potential uses for data sets are discovered that have already undergone a previous framework review. In addition, since the vast majority of the data that may be subjected to a framework review will be stored, accessed, and analyzed in the digital world, it is important that well-established cybersecurity frameworks and data-handling best practices are utilized to ensure the security of the new data sets.

Conclusion

Law enforcement agencies at all levels of government -- local, state, and federal -- strive to do their best to protect our citizens, their wellbeing and their property, from all manners of threats and criminal activities. We can best succeed in meeting this objective by ensuring that the tools at our disposal continue to meet our needs and serve the best interests of the community. I believe the recommendations I have outlined above cover two key issues that must be addressed by law enforcement in order to successfully identify and integrate new technologies and methodologies into our procedures and work flows.

Chief Bill Partridge

City of Oxford, Alabama

Bill Partridge has served the citizens of Oxford since 1989. Prior to becoming the Chief of Police, Bill served as Operations Captain for the police department, supervising the uniform division and special operations. He has held every rank in the police department with the exception of Assistant Chief. He is a Crash Reconstructionist and instructor in media relations, law enforcement technology, crash investigations and special event planning to mention a few. He also served as Calhoun County Coroner from 2001-2006.

Chief Partridge serves on numerous boards in the field of law enforcement and public safety, to include Alabama Peace Officers Standards and Training Commission as vice-chairman. He is currently President of the Alabama Association of Chiefs of Police, and is the board chairman for the Center for Best Practices in Law Enforcement at Jacksonville State University.

Chief Partridge holds a graduate certificate in Criminal Justice from the University of Virginia and has attended the University of North Florida's Institute of Police Technology and Management. He is also a graduate of the 225th Session of the FBI Academy in Quantico, Virginia. He is a Certified Law Enforcement Executive by the Alabama Peace Officers Standards and Training Commission, and a Certified Chief of Police.

Bill Partridge
Chief of Police
City of Oxford, Alabama

Crime Centers for smaller agencies and regions to fight crime

The East Metro Area Crime Center (EMACC) Explained.

In short, the Crime Center provides vital technology and intel to the region, thus saving time and manpower to solve and prevent crime. The Center consists of twenty-eight local, state and federal agencies from across the region, all working together under one roof, to accomplish this mission.

The East Metro Area Crime Center (EMACC) uses and shares advanced technology with its regional partners, including, but not limited to: pole cameras, camera trailers, license plate readers (LPR), crime tracing software, phone and computer forensics (Cyber Crimes Lab) facial recognition software. The Center uses a large video wall inside the video center to monitor cameras which are placed throughout the region on poles and camera trailers; on-site gunshot detection and shell casing analysis help to further reduce gun crimes in the region. Child crimes are also investigated through the cyber-crimes unit located within the Crime Center.

The Center not only monitors cameras in the region, but also utilizes cameras located at financial institutions and school systems throughout the area. Pulling live feed from these cameras into the video center at the EMACC allows for the immediate relay of real-time information to school SRO's and police officers responding to emergency calls. This real-time information saves time and gives the officers much needed live information to stop active shooters or other crimes that are in progress. Cameras located at financial institutions allow the video

center to deliver instantaneous information when robbery alarms are activated, and provide descriptions and weapons information to responding officers.

Since its creation in May of 2019, the East Metro Area Crime Center has celebrated much success throughout the region. This includes solving Bank Robberies within minutes of the robbery; numerous homicides, and cold case homicides; home invasions, burglaries over a five county region, and car theft rings; also violent crimes, including gun crimes which were linked by shell casings to multiple shootings and homicides.

By having twenty-eight agencies actively involved in the Crime Center, we have seen significant crime reductions; some as much as double digit crime reductions. The Center's greatest success is the sharing of information across the region with other law enforcement agencies. This is something that wasn't practiced very well prior to the implementation of The Center.
The success of the EMACC in Oxford, Alabama has led to the creation of others within the state. We are linking these centers together as they come on-line.

Often, you only think of large urban cities implementing Real-Time Crime Centers; in which case, one single agency utilizes the technology. By building Crime Centers in smaller areas and having multiple departments utilize the center's technology, law enforcement has found we can multiply the man power and solve crimes on a larger scale, thus keeping the communities safer with less man power. Larger cities, with more populous areas, have abundant technology to help solve and prevent crime. This is an advantage smaller, more rural areas don't have. Most small police departments and sheriff's departments do not have the allocated funding required to utilize technology the way the EMACC does to prevent and solve crime. Our Center doesn't charge participating agencies for taking part. We only ask that they provide manpower if possible.

This cohesive concept can provide significant technology to rural areas and much smaller agencies. The Oxford Police Department is fortunate to have a mayor and city council willing to implement this center and fund it. With that being said, the use of federal grant dollars on a regional scale as opposed to individual agency use, would allow for the creation of crime centers across the county and help multiple agencies in solving and preventing crime.

The East Metro Area Crime Center serves a multiple county region consisting of twenty-eight agencies which serve approximately 300,000 citizens. I invite any member of the commission, or the commission as a whole, to visit the EMACC and see how we are implementing technology on a regional scale to fight and solve crime.

Christopher Amon

Chief, Firearms Operations Division Bureau of Alcohol, Tobacco, Firearms and Explosives

Christopher Amon has been the Chief of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Firearms Operations Division since February of 2019. In this role, Special Agent Amon oversees the National Integrated Ballistics Information Network (NIBIN), the NIBIN National Correlation and Training Center (NNCTC), and ATF's Crime Gun Intelligence Programs. He is also the Chairman of the National Crime Gun Intelligence Governing Board, which consists of Chiefs of Police, United States Attorneys, District Attorneys, and Laboratory Directors from Major Cities who advise ATF on policies related to Crime Gun Intelligence.

Chief Amon began his career as an ATF Special Agent in the Denver Field Division in 2005. He worked on violent crime investigations and firearms trafficking by criminal organizations. He also was a part-time member of ATF's Los Angeles Special Response Team, where he served as a crisis negotiator.

In 2012, he moved to ATF Headquarters in Washington, D.C., where he worked in Public and Governmental Affairs. In this role, Special Agent Amon regularly briefed members of Congress and provided technical assistance in drafting legislation.

In 2015, Special Agent Amon returned to the field as the Group Supervisor in the Denver Field Division's Crime Gun Intelligence Center (CGIC) –a task force using NIBIN technology and a dedicated investigative team to identify shooters and crime gun sources.

Prior to his role at ATF, Special Agent Amon served as a congressional aide on Capitol Hill. He holds a Bachelor's Degree from Fordham University in the Bronx, New York, and a Master's Degree in Professional Studies from George Washington University in Washington, D.C. He is a native of Brooklyn, N.Y.

U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Firearms Operations Division

Testimony of Special Agent Christopher C. Amon
Chief, Firearms Operations Division
Bureau of Alcohol, Tobacco, Firearms and Explosives
For the Presidential Commission on Law Enforcement and the Administration of Justice
April 16, 2020

Good afternoon, it is my distinct honor and privilege to address the Commission. My name is Christopher Amon, and I serve as the Chief of the ATF Firearms Operations Division. In this role, I oversee the National Integrated Ballistic Information Network (NIBIN), NIBIN National Correlation and Training Center (NNCTC), and Crime Gun Intelligence (CGI) programs. Prior to this role, I served as the Group Supervisor of the Denver Crime Gun Intelligence Center (CGIC) where I oversaw investigations of violent crimes using CGI.

Of the more than 390 million firearms in America, most will never fall into criminal hands. Law enforcement must use our limited resources to focus on the fraction of firearms used in crimes. CGI is the collection and analysis of all available information related to the unlawful use, possession and/or transfer of these firearms. These details help investigators identify individuals or groups committing acts of firearm violence, illegally diverting firearms, or both.

The foundation of a CGI program is technology. Participation from stakeholders in both NIBIN and E-Trace allows investigators to identify crime guns using cutting edge technology and trace their origin quickly. Processing crime gun evidence starts at the scene with comprehensive collection and continues when evidence arrives at a laboratory or NIBIN site. Timely analysis of ballistic evidence is critical for providing leads to solve shootings and stop future ones.

As law enforcement, we must prioritize shootings and sources of crime guns. Academic studies of shooting events linked by NIBIN show there is a high likelihood for reoccurring gun violence within a short period of time. NIBIN results also illustrate a progression of violence in which an unlawful discharge of a firearm progresses to a shooting into a residence, and later an aggravated assault or homicide.

Law enforcement officers must race against time to identify and prosecute shooters before they can reoffend. Technology is proving to be our best match for the speed of repeat gun violence. By entering evidence quickly into the NIBIN system, investigators can catalogue events in near real time, accruing a wealth of investigative leads.

NIBIN Technology

The NIBIN network is a collection of digital ballistic images of ammunition components recovered from crime scenes and recovered crime gun test fires. Like fingerprints, every firearm produces unique identifying characteristics when fired. The barrel of a weapon leaves distinct markings on a bullet or projectile, and the breech, firing pin and ejector mechanisms leave distinct markings on the cartridge case. When analyzing bullets and cartridge cases, firearm examiners and technicians

use these markings to determine if ballistic evidence was expelled from the same firearm. For the purposes of this testimony, I will discuss the capabilities related to cartridge cases, not projectiles.

NIBIN was established in 1997 as the merger between two ballistic imaging/identification programs: the FBI's Drugfire and ATF's Ceasefire. In 1999, a single technology—the Integrated Ballistic Identification System (IBIS) under Ceasefire—was selected to provide nationwide support for the NIBIN network and has served this role ever since. In 2003, ATF took sole responsibility over the administration of the NIBIN, both the technology and network infrastructure.

At the start, investigators principally used NIBIN as a back-end forensic tool to confirm a link they knew existed between two or more violent crimes. Success was sporadic. In 2012, technology upgrades from 2D images to High Definition 3D spurred investigators to use NIBIN as a front-end, lead-generating tool. The technological advancement allowed NIBIN technicians and Firearms Examiners to better view similarities on the "Regions of Interest"—the areas where firearms leave unique markings on cartridge cases. Now, technicians could confidently establish an unconfirmed NIBIN "lead" and allow investigators to generate solid connections without waiting for microscopic confirmation. Additionally, some NIBIN sites who did not put out investigative leads had their examiners conduct microscopic analysis within days, giving investigators a confirmed hit in a short period of time. Cities like Denver also saw success by collecting and entering all cartridge cases, including for victimless crimes not normally prioritized. This is where the principle of "comprehensive collection" was born.

ATF recognized NIBIN's enormous potential. Following an analysis of best practices during this time period, ATF created the four critical steps of NIBIN: **Comprehensive Collection, Timely Turnaround, Follow-up, and Feedback**.

Comprehensive collection is the foundation of NIBIN. Partner agencies must collect and submit all evidence suitable for entry into NIBIN, regardless of the severity of a crime. Evidence includes cartridge cases recovered from crime scenes and test fires from recovered crime guns. Shooting events tend to escalate, so it is imperative to institute agency policies to recover all suitable ballistic evidence from crime scenes and process it through NIBIN. Low priority shooting events routinely link with higher priority events. Law enforcement should prioritize a victimless shots fired call with the same urgency and attention as a homicide case.

Timely turnaround is crucial, as violent crime investigations turn cold fast. As a result, timely intelligence gained through NIBIN is critical to solving violent crimes and stopping violent offenders before they can reoffend. Quick turnaround during all phases of NIBIN analysis, including the entry and acquisition into NIBIN, correlation reviews, and the dissemination of NIBIN leads, is vital.

ATF developed the NNCTC in 2016 to assist with timeliness. Located in Huntsville, Alabama, the NNCTC provides ballistic image correlation review, the most time-consuming step within NIBIN, to more than 75 NIBIN sites throughout the country. The NNCTC develops leads and returns them within 48 hours. Since March of 2016, the NNCTC has conducted approximately 263,000 reviews and provided more than 67,000 investigative leads to partner sites.

In addition, ATF also created the NIBIN Minimum Required Operating Standards (MROS) to improve timeliness and consistency across the network. The MROS require all sites who participate in NIBIN to enter eligible evidence within 2 business days of receipt, conduct a correlation review within 2 business days (does not apply if an NNCTC site), and distribute leads to investigators within 24 hours.

Best Practices Lead to Increased Participation and Outputs

Ensuring comprehensive collection and creating policies to improve the NIBIN program have yielded exponential growth:

FY	2014	2015	2016	2017	2018	2019	2020
Leads	800+	6,300+	19,600+	41,000+	47,000+	67,000+	85,000+*

*Projected

During this same time period, acquisitions increased from 205,000 in FY15 to more than 384,000 in FY19. In FY14 there were 170 NIBIN sites. In FY20 we project finishing with 240 sites.

This is a significant move forward for the program. Leads represent new investigative avenues for law enforcement to focus efforts and take active shooters off the street. With only 800 leads nationwide in FY2014, there was limited need for organizations to change course. That has now changed.

Investigative Efforts-Crime Gun Intelligence Centers/Enforcement Teams

In 2016, recognizing the overall increase in valuable CGI and NIBIN leads, ATF established 25 CGICs, strategically located across the nation to provide investigative leads and support to CGI initiatives. These CGICs collect, analyze, and triage the multitude of intelligence from NIBIN, e-Trace, and other sources to produce actionable intelligence for investigators.

In 2017, the Bureau of Justice Assistance (BJA) adopted the ATF CGIC concept as an avenue for State/Local law enforcement to pursue funding and promote the CGIC initiative. The guiding principle of these strategies is to provide focused investigative efforts on the hundreds or thousands of crime gun leads generated within a given Area of Responsibility (AOR).

In 2017, The MITRE Corporation studied ATF's CGICs and the CGIC concept. One of their key findings suggests dedicated investigative teams only pursuing NIBIN leads have the greatest return on investment and achieve more frequent successes. ATF agreed with this finding and established Crime Gun Enforcement Teams (CGETs) dedicated solely to leads developed by the CGIC.

CGICs partner with CGETs to provide dedicated intelligence-driven targeting of violent offenders and timely follow-up of CGI leads through well-established protocols. These teams devote efforts to immediate follow-up of NIBIN/CGI leads and the interdiction of shooters, yielding impactful results.

Results

Through commitment and partnerships, the steps described above have already yielded impressive results. Since March of 2018, ATF has cataloged more than 1,000 success stories across the country where NIBIN produced better investigative outcomes. Here are a few examples:

- In Baltimore, MD, the CGIC, working with the Baltimore Police Department, identified an individual responsible for two attempted murders occurring within a 30-day timeframe. In the first incident, the individual shot someone he believed followed him in his vehicle. In the second incident, he shot someone at his former workplace. Cartridge cases recovered from both scenes were placed into NIBIN and immediately linked, which allowed investigators to obtain a search warrant for the suspect and recover the firearm tracked through NIBIN. This individual pled guilty to numerous Federal firearms violations. **The key takeaway** in this case is the importance of a timely NIBIN process to disrupt shooters. A delay in discovering the link could have resulted in more shooting events.

- In Newport News, VA, ATF and its partners used NIBIN to link multiple shooting events tied to two feuding local street gangs. These shootings left a 13-year-old dead at a birthday party and resulted in another gang-related homicide. During an 8-week trial, the Government presented NIBIN-related evidence linking these shootings. The NIBIN links persuaded several defendants to cooperate and corroborated statements from witnesses. **The key takeaway** is the importance of using NIBIN and CGI to establish a pattern of violence perpetrated by criminal organizations to ensure prosecutions capture the totality of their violence.

- In Detroit, MI, the ATF/DPD CGET, acting on leads generated by the CGIC, reviewed three victimless "shots fired" calls linked by NIBIN. Investigators used CGI to identify a potential suspect as an individual known to shoot at rival gang members. The CGET team executed a search warrant at the suspect's girlfriend's home and recovered the firearm used in the shootings. The NIBIN links were presented during the detention hearing and the suspect was held without bond. **The key takeaway** is the importance of a team dedicated to investigating NIBIN links. Without a dedicated team, these three different "shots fired" incidents may not have been prioritized. The Detroit CGET focused solely on these links and employed CGI techniques to identify a suspect. As a result, a judge denied bond in a firearm possession case.

Other Technologies/Forensic DNA

Acoustic Gunfire Detection Systems are a force multiplier for NIBIN/CGI programs. Among other benefits, an acoustic gunshot detection system helps cities increase evidence submission into NIBIN, allowing CGICs to receive new NIBIN leads. By detecting gunfire –especially in the absence of a 9-1-1 call –officers can respond and recover cartridge cases quickly.

Automatic Evidence Analysis software helps investigators manage a mountain of probative evidence. Social media search warrant returns, cell phone records, and other digital evidence often require analysts to spend hours generating connections. There are several promising private sector solutions that automate this laborious process so results can be analyzed and visualized within minutes.

New Techniques to recover DNA from Fired Cartridge Cases: Recently, the ATF National Laboratory developed a process to preserve and recover DNA profiles from fired cartridge cases (FCC) while also meeting the 2-day requirement for NIBIN entry. This in-lab extraction procedure can be easily implemented into any laboratory's current workflow. While previous studies indicated low success rates extracting usable DNA profiles, our DNA section implemented innovative methods that have yielded promising results. In one case in San Francisco, DNA recovered from 18 fired cartridge cases led to the identification and arrest of two murder suspects connected by NIBIN to additional shootings. Extracting DNA in every case is not feasible, but when the only evidence is fired cartridge cases, the investment in high-quality processes secures an indisputable way to identify a suspect in crime gun investigations. Currently, ATF's DNA success rate is as follows:

- Approximately 30% of the time a usable and identifiable DNA profile is recovered from a fired cartridge case,
- Approximately 75% of the time a usable and identifiable DNA profile is recovered from at least one of the FCCs within a group assumed to have originated from the same firearm.

Recommendations:

- All U.S. law enforcement agencies should participate in NIBIN. Law enforcement executives should work with elected officials to mandate NIBIN participation via state law in a manner resembling rape kit testing laws.
- Law enforcement agencies should mandate collection of all fired cartridge cases and test fires from all recovered firearms.
- ATF and law enforcement agencies should work together to establish dedicated investigative assets to target shooters using CGI. Shooters know no jurisdictional bounds, neither should law enforcement.
- When NIBIN sites join the network, lead agencies should establish a plan to implement NIBIN Minimum Required Operating Standards prior to launching the technology.
- Utilize ATF's DNA tool to help solve violent crime through grants to state and local laboratories designed to add more scientists, grow the facilities' footprint, and fund additional instruments. Additionally, we need to expand our federal laboratories to meet the need for the federal caseload.
- Law Enforcement agencies should establish regional stakeholder meetings to ensure all participating agencies utilize CGI best practices.
- Invest in software for investigators to aggregate and analyze different CGI sources (ex: NIBIN, ShotSpotter, Social Media, cell tower analysis).

In summary, the investigative results from dedicated NIBIN efforts prove this technology has revolutionized crime gun investigations and prosecutions. Rather than following a trail of bloodshed, investigators can track gun crime in real time and intervene before lives are lost.

Assistant Chief David LeValley

Detroit Police Department

Assistant Chief David LeValley is a 25 year veteran of the Detroit Police Department. Throughout his career, he has held a variety of assignments within the department, including patrol, administration, and detective functions. He was appointed to his current rank of Assistant Chief in 2018. Assistant Chief LeValley currently oversees the Office of Neighborhood Policing, which includes operations at all of the city's eleven police precincts, Downtown Services, Metropolitan Division, Gaming, and the Detective Bureau. Assistant Chief LeValley holds a bachelor's degree in Public Safety Administration from Eastern Michigan University and a Master's of Business Administration from Wayne State University. He is a graduate of the 240th session of the FBI National Academy.

Leveraging Technology to Reduce Crime

DAVID LEVALLEY, ASSISTANT CHIEF OF POLICE
DETROIT, MICHIGAN POLICE DEPARTMENT
LEVALLEYD711@DETROITMI.GOV

April 16, 2020

David LeValley, Assistant Chief of Police
Detroit, Michigan Police Department

Leveraging Technology to Reduce Crime

The city of Detroit has historically experienced crime rates much higher than the national average. While studying crime in Detroit, and in particular the high number of robberies and carjackings that were occurring, we found that there was a significant problem at gas stations and liquor stores throughout the city. Much of the crime was occurring after dark in the parking lots of those businesses. We also discovered that many of these predatory crimes of robbery and carjacking went unsolved. The Detroit Police Department had tried a variety of unsuccessful projects in the past to deter crime. Most of these projects involved police officers conducting street enforcement operations, in which we used forfeiture funds to pay officers overtime to make arrests in high crime areas. However, we found our reactionary efforts had no significant impact on reducing overall crime or changing behavior.

We began to look for a proactive way to create what we believed would be safe places for our citizens to visit and conduct business. We also wanted to ensure that when a crime did occur at one of those locations, there was a greater likelihood that we would be able to solve the crime. We looked toward available technology, along with community partnerships to create a multi-faceted approach to address violent crime at targeted locations. In early 2016, we implemented Project Green Light Detroit, coupled with comprehensive License Plate Reader and Facial Recognition programs to address the issue. As a result, violent crime in Detroit has dropped 16% comparing 2015 to 2019. There were 35% fewer robberies and 53% fewer carjackings in Detroit during 2019 than in 2015. Robberies dropped from 3,648 in 2015 to 2,377 in 2019 and carjackings dropped from 523 in 2015 to 244 in 2019.

Project Green Light Detroit

As the city was beginning to see growth and development in areas it had not seen for years, the Detroit Police Department knew it was critical to create innovative ways to strategically combat crime at our most high-risk locations. Internal analysis showed a significant amount of violent crime was occurring at or near city gas stations and liquor stores. Therefore, it became clear that the department needed to target their crime-fighting efforts toward these areas. From this, the idea resulted in the development of a unique program called Project Green Light Detroit, a new and innovative program, enlisting local business owner's assistance to combat the disproportionate amount of crime occurring in and around their businesses. The program, which is managed by the Detroit Police Department, is the first-ever public-private community partnership of its kind, blending a mix of real-time crime-fighting and community policing aimed at improving neighborhood safety, promoting the revitalization and growth of local businesses, and strengthening our efforts to deter, identify, and solve crime. As part of the program, Detroit business owners volunteer to install high definition camera systems at their businesses and allow video feeds to be viewed in real-time, at the Detroit Police Department's Real-Time Crime Center. This allows officers the ability to provide an immediate virtual response to issues at their business, as well as review camera footage to assist in criminal investigations.

In January of 2016, the Detroit Police Department piloted the program by partnering with eight gas station owners who volunteered, at their own expense, to install high definition cameras in strategic areas of their business, capturing areas that are accessible to the public. These video feeds are sent in real-time to the Detroit Police Department's Real-Time Crime Center, where they are monitored by crime analysts and police officers. Feeds are also available to be viewed, after the fact, to assist with criminal

investigations. In addition to allowing the Detroit Police Department access to the camera feeds, businesses are required to maintain 30 days of video storage, along with posting signage in and around their building indicating the business is monitored by police. Owners must also install a green flashing light outside of the business as a beacon to customers and criminals, informing them that the business participates in Project Green Light. Combined, they act as a deterrent to those who may consider committing a crime at the location and identify the business as a partner of the Detroit Police Department.

Since the pilot, the project has experienced significant growth. Today 699 businesses are participating in the program, giving department members access to over 2,800 live camera feeds throughout the city. There are also a significant number of businesses in the pipeline waiting to join the program. Efforts to bring these businesses and more into the program are fueled by the belief that the more businesses in the program, the higher the reduction in crime will be.

With camera feeds being monitored at the Real-Time Crime Center, as well as at all precincts, members can proactively patrol the business virtually to identify issues requiring additional police response. Department members also perform a virtual response to all calls for service at any Project Green Light location. This means that any 911 call initiated from a participating business will automatically have personnel at the Real-Time Crime Center monitor the video feeds. Personnel are required to view and appropriately respond to any issues at the location, thus providing actionable intelligence gathered from the video to responding officers on the street. This has enhanced officer safety and improved our response to citizens in distress.

The program also requires officers on the street to make extra patrol visits to participating businesses during their normal tour of duty. Officers spend time inside and in the parking lot of the business being more visible to the public, creating a safer environment at the location. This helps to build relationships with the community and the owners themselves when they see and interact with officers on a more recurring basis. The frequency of officer presence at these businesses is increased, which not only acts as a crime deterrent, but has also been reported to increase their customer traffic.

Detectives throughout the department are using Project Green Light video feeds to assist in case closure as well. There have been hundreds of cases solved through the use of this video footage. Efforts are now underway to statistically understand the effects of Project Green Light on case closure, but case after case has proven that having immediate access to business video feeds has been essential to our ability to react quickly to violent incidents and taking offenders into custody.

According to a recent analysis conducted by the Project Green Light team, the original eight participating businesses have experienced an overall reduction of violent crime of 44.9% when comparing 2015 (before Project Green Light) to 2019. All participating gas stations and liquor stores have seen a reduction of 25.3% and 18.2%, respectively, in the same time frame. Michigan State University is the research partner for Project Green Light. It is expected that the results of their research will be concluded by the end of this year.

License Plate Readers

Part of the technology package that the Detroit Police Department invested in includes a network of license plate readers throughout the city. The License Plate Reader (LPR) provides automated detection of license plates by deploying a high-speed camera, mounted either at a fixed location or on a

mobile patrol vehicle. A computer then compares data from electronic images of vehicle license plates against specified databases of license plates. The system captures data about the image, such as camera identification, date, time, and GPS coordinates, as well as data about the vehicle, including the vehicle's make and model, the vehicle's driver and passenger(s), distinguishing features (e.g., bumper stickers, damage); and state of registration.

The license plate readers compare against two databases of license plates, otherwise known as "hot lists." One is maintained by the FBI's National Crime Information Center (NCIC), which contains information about wanted vehicles and persons nationwide. DPD also maintains a "local hot list," which consists of vehicle plate information entered by members of DPD. This is used for vehicles that are known to be used in violent crimes. License plates entered into the local hot list are automatically purged within 24 hours and must be re-entered if needed. When the system registers a match with one of the hot lists, department members are alerted and able to quickly locate wanted vehicles and people.

Additionally important is the investigative value in the data that is collected by the license plate readers. After a crime has occurred, department members are able to access the system to verify the location of a vehicle that has passed one of the many stationary or mobile license plate readers located throughout the city. This information is valuable in proving that a vehicle was either present or in close proximity to a crime scene.

Facial Recognition

One of the most controversial, but tremendously valuable pieces of technology that the Detroit Police Department uses in combating violent crime is Facial Recognition software. In 2017, the department began using facial recognition software in our Crime Intelligence Unit. Since that time, we have developed positive investigative leads in 276 instances, or 41% of the time facial recognition is used.

When a violent, part one crime (Homicide, Aggravated Assault, Robbery, or Rape) occurs that is captured on video or an image of a suspect is available, analysts trained by the FBI evaluate the probe image for use in the facial recognition system. The analyst then enters that image into the facial recognition system, which compares the image to a database of local mug shots for a potential match. The system returns numerous mug shots of possible candidates and ranks them in the likelihood of matching the probe image. Once the analyst identifies who they believe to be a probable match, it is reviewed by another trained analyst and a supervisor must then concur before an investigative lead is sent out. It is important to note that in addition to the automated system match, the analysts use other available resources to verify the investigative lead, such as reviewing social media pages for recent photographs revealing vehicles and clothing, or conducting a review of prior police reports involving the individual. Also, this information only provides an investigative lead for detectives to use and does not constitute probable cause to make an arrest. Detectives must still establish probable cause with other independent evidence before an arrest can be made.

We initially received a considerable amount of public protest regarding our use of facial recognition technology. There were many misconceptions surrounding the way this technology was used by the Detroit Police Department. The department does not use facial recognition on live video feeds to identify individuals, for any kind of predictive analytics, nor for the purpose of conducting surveillance on any individuals, and we do not rely solely on the software's algorithm to make an identification. We have a diverse group of trained analysts who conduct facial recognition searches. We have found that it is

important to have a comprehensive and strict policy on the use of the technology to ensure that no citizen is wrongly identified or convicted of a crime based on the improper use of the technology. To date, we have no such instances on record.

Success Stories

In May 2019, police responded to a home in which three individuals were shot and killed by a masked gunman. There were two other individuals present, but they were unable to identify the suspect. In re-tracing the steps of the homicide victims prior to their death, detectives were able to determine that all three were at a Project Green Light Detroit gas station earlier in the evening. The victims met up with a fourth individual, later identified as the suspect, on camera and then left the location together. After an altercation at the crime scene, the suspect left the location upset and embarrassed, later returning to shoot them. Analysts were able to use the high definition footage to enter the person's image into our facial recognition software. They ultimately produced an investigative lead and a canvass of the area surrounding the suspect's home produced video footage of the suspect running home in a mask after the murders had occurred. The suspect was arrested and was ultimately convicted of the murders. Without the use of this technology, detectives never would have known to canvass for video near the suspect's home and he may have never been identified.

In September 2019, an analyst from the Detroit Police Department was reviewing a live Project Green Light camera feed from a local gas station when the analyst observed an armed robbery and non-fatal shooting take place in the parking lot. The analyst alerted patrol units who responded to the scene, but the suspect had fled by the time they arrived. The analyst was able to quickly obtain a photograph of the suspect's face and his vehicle from the high definition Project Green Light cameras. The analyst entered the suspect's image into our facial recognition system and produced a potential lead. The analyst was then able to determine that the suspect had a vehicle registered to him, which matched the vehicle that fled the crime scene. The analyst used our License Plate Readers to determine that vehicle was in the close proximity of the crime scene. The lead was passed on to detectives and the suspect was ultimately identified by the victim, later arrested, and has been convicted of Armed Robbery and Assault with Intent to Murder. Without the use of these three pieces of technology, the suspect may have very well gone unidentified and remained on the streets to victimize other citizens.

These are just two examples of the successful use of this technology, but these stories repeat themselves over and over throughout the city of Detroit.

Recommendation

The Detroit Police Department has been successful in reducing and solving crime through the use of these three strategies and are now implementing a considerable technology expansion plan. The city of Detroit is currently in the process of significantly expanding our camera assets, adding almost 1,000 traffic cameras at intersections that the police department will have access to. We are also installing additional cameras and License Plate Readers along the highest crime corridors throughout the city that will be monitored at precinct level intelligence centers, which are currently being built inside of the department's busiest precincts.

Based on our experience and the lessons learned, I am making the following recommendations to the panel with regard to the use of technology to reduce or solve crime:

- **Invest in technology infrastructure** – Investment in a robust technology infrastructure is critical to the success of any large scale deployment. It is also important to continue to evaluate for necessary improvements to create a sustainable program. We were fortunate to have a good team in place that was willing to take risks on unconventional projects which paid off. Funding must be identified to support the growth and expansion in any departmental technologies as well. This can obviously be difficult for many agencies, but it is critical for success.
- **Encourage transparency** – Having complete transparency in the planning and development of our programming has been key. We publicly discuss our successes, challenges, and failures in an effort to show our own growth. We have opened the department for tours to public officials, media, and key stakeholders in the community to ensure we keep them informed. As any department contemplates these efforts, it is highly advised to take this approach. It is easier to be open and straight forward at the beginning of any undertaking like this.
- **Mandate training and certifications** – Regardless of all the technology that can be purchased, there will always be a requirement for human intervention to ensure their safe and efficient use. We have learned how valuable this has been in defending our facial recognition program. Mandating universal certifications and training will protect both law enforcement agencies and the public from misuse.
- **Increase technical assistance** – When we began exploring the idea of making a considerable investment in technology to combat crime, we toured several police agencies throughout the country in an effort to collect as many of the "best practices" on the topic that we could. Facilitating technical assistance and peer exchanges with other law enforcement agencies to understand their "best practices" and lessons learned would be useful.
- **Keep CJIS up to date with current technology** – One of our largest and continuing challenges is keeping within Criminal Justice Information Systems (CJIS) guidelines with new technologies and projects. It is recommended to identify personnel dedicated to investigating the impact of any technological upgrades to CJIS compliance. Without this, police agencies will have difficulty maintaining compliance when purchasing new technology, much of which has advanced beyond the limitations of CJIS.
- **Be willing to take risks and test proofs of concept** – Buy in from government officials and support from community leaders has been valuable to us as our project needs have grown. This support has allowed us to focus on and meet our overall goals for improving crime rates and the quality of life for those in the city. Buy in from all levels in the police department has been challenging, but was accomplished through a cultural shift and by providing front line officers with much improved technologies as well.