Chapter 6. Technology

Introduction of the Issue

"The advances in various technologies are having the most dramatic impact on the way we do business since [he] began nearly 50 years ago![1]" - Sheriff Al Cannon

Advances in consumer product technologies have created opportunities and efficiencies in many aspects of daily life. Such advances have spawned new forms of connectivity through social media, bringing people around the world together in ways not imagined or technologically possible just a few decades ago. As the law-abiding public has embraced these technologies, they have nurtured innovation even further and spurred a transformation of commerce and communication; however, at the same time, these technologies have opened a new world for exploitation by criminals, terrorists, and spies.

Attorney General William P. Barr, spoke to this concern at the Lawful Access Summit in Washington, DC, in October 2019:

> But the digital world that has proven such a boon in many ways has also empowered criminals. Like everybody else, criminals of all stripes increasingly rely on wireless communications, hand-held devices, and the internet. In today's world, evidence of crime is increasingly digital evidence. As we work to secure our data and communications from hackers, we must recognize that our citizens face a far broader array of threats. Hackers are a danger, but so are violent criminals, terrorists, drug traffickers, human traffickers, fraudsters, and sexual predators. While 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. In other words, making our virtual world more secure should not come at the expense of making us more vulnerable in the real world.[2]

Emerging technologies have an impact on law enforcement in two primary ways. Emerging technologies present great opportunity to increase law enforcement capacity and aid in the efficient use of public funds while enhancing law enforcement's ability to identify victims and bring perpetrators of crime to justice. At the same time, risks and costs associated with the adoption of new technologies must be addressed prior to use by law enforcement. Technologies can enhance, enable, or better facilitate a law enforcement agency's mission by

- improving public, department, and officer communications
- reducing response time
- improving command and control structures
- expanding domain awareness
- ensuring officer safety and regulatory compliance
- enhancing evidence-gathering capabilities

Conversely, law enforcement agencies who use available technologies without appropriate restraints will negatively affect both the mission and public trust. These risks, threats, and costs contribute greatly to the complex environment in which modern police agencies work.

While some perceive the influx of information available through modern technological means makes law enforcement's job easier, the law enforcement environment related to the collection of information and deployment of technology is far more complex. Law enforcement operates in accordance with the rule of law under Constitutional and statutory restraints that impose limits on police authority consistent with the

[1] Al Cannon, Sheriff, Charlestown County, In discussion with Technology Working Group,)
[2] William P. Barr, Remarks as Prepared for Delivery, Lawful Access Summit, Washington, DC, October 4, 2019).

public will. In some cases, information that is readily available to the public may not necessarily be available to law enforcement agencies. Emerging technologies that can be deployed to assist law enforcement may also be deployed to interfere with, threaten, or even harm law enforcement activities and personnel. Public trust in police agencies can turn quickly if there is a perception of abuse or misuse of technology or personal data. While assessing the risks and costs associated with the deployment of new technology or acquisition of information, law enforcement agencies must also be aware of the impact their actions have upon, and the relationships they have with, their communities.

The commission's working group developed, considered and tested two frameworks: one for adopting new technologies and one for the handling and use of data. Each framework, broken up into areas of consideration, offers a starting point for law enforcement executives to identify the most critical concerns and the specific considerations necessary to help assess whether a law enforcement agency should implement a technology or data enabled capability.[3] These frameworks offer law enforcement executives the flexibility to address specific issues that they recognize as most important in their unique circumstances. These frameworks will evolve over time as law enforcement faces challenges and opportunities and as new, innovative, and developing technologies are available for use by law enforcement or deployed for use by criminals to counter law enforcement objectives.

The term "framework" represents a carefully considered, methodical, and repeatable approach law enforcement agencies may use to consider the generation or acquisition of a new dataset or the adoption of a new technology. The intention of these frameworks is to help guide law enforcement executives through decision-making processes, assessing the pros, cons, and other predictable considerations. The commission proposes the attached frameworks as a starting point, understanding that they will be refined to encompass a broader range of technology and data types and allow questions to evolve as agencies gain experience in the process. These frameworks are not intended as a checklist where all questions must be answered each time. Rather, only the applicable questions necessary need to be considered for a particular technology or data set.

In the implementation phase, the framework questions are designed to help agencies consider how they can best implement a technology, ingest a new data set and further identify the attendant consequences. For example, the question may be raised, how can agencies ensure the use of the technology is not perceived as being overly intrusive? This may be done through training, education, outreach, and communications with the public. It may also lead to limiting the use of the technology through technical methods or auditing to address concerns unique to a law enforcement executive's own constituency.

The commission recognized it could not address all of the possible iterations and applications of various technologies or datasets. Instead, the commission addressed themes that transcend the deployment of individual technologies or acquisition of different data sets while highlighting some of the most common technological challenges faced by law enforcement agencies today.

6.1 Implementing New Technologies

PULL QUOTE: "Technology plays an undeniably critical role in various facets of our modern society, and law enforcement is no exception. Nearly every crime suppression and prevention strategy now involves technology, and we have seen increased success with many of these approaches due to technological innovations and advancement." - Robert J. Tracy, Chief of Police (Wilmington, Delaware); former Chief of Crime Control Strategies (Chicago Police Department), retired Captain (New York City Police Department)

Background

There has always been an inevitable, but necessary connection between law enforcement and the field of technology. Law enforcement professionals are constantly inundated with new technologies at an alarming rate. This creates an ongoing issue where law enforcement must then sift through the onslaught of innovative technologies and advancements to previously developed technologies.

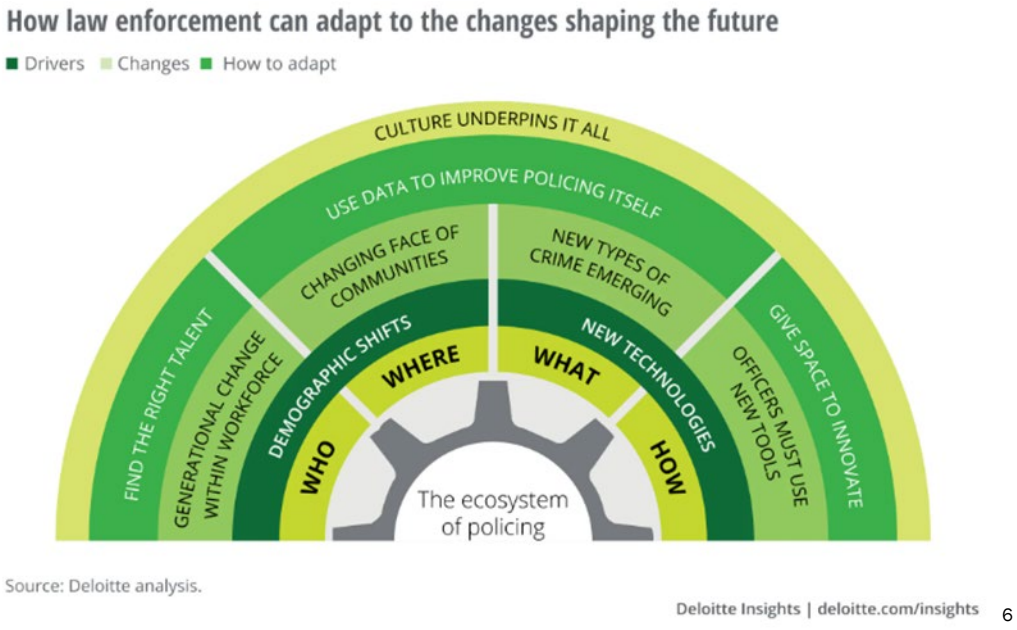
[3] Memory, "From 'Data-Driven' to 'Data-Enabled,'" Timely Blog (blog), October 22, 2018, https://memory.ai/timely-blog/from-data-driven-to-data-enabled.

It can be difficult for even the largest law enforcement agencies to introduce and adopt new technologies, and when they do adopt them, the increased scale of the larger agencies can make implementation a challenge. In addition to the pace of technological development, the acquisition of new technologies presents significant costs in the face of financial and budgetary constraints. Deployment of new technologies also raises other significant issues for consideration, including public acceptance and that the technology is being deployed and information being obtained by law enforcement is accomplished within the appropriate Constitutional and legal framework.

Current State of the Issue

While the law enforcement field has seen a rise in a younger, digital native workforce in recent years, law enforcement agencies may lack the necessary resources (e.g., personnel, facilities, or advanced computing experience) to make fully-informed and prudent decisions regarding the adoption of advanced, new, or emerging technologies. [4] [5] Agencies may also lack a framework to properly test and evaluate short and long-range implications of technology adoption. The limited ability of many agencies to compete with the private sector in hiring or retaining employees with technological expertise intensifies this challenge.

The prevalence of technology among law enforcement agencies is undisputed. The current climate of the emergence of new crimes (e.g., those found on the dark web) and the vast amounts of data available to law enforcement, coupled with generational changes in the workforce and community needs, necessitates the use of new technologies.



[4] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Rural and Tribal Topic: Challenges Law Enforcement Face in Rural Areas, Before the Commission (May 19, 2020) (written statement of Michael A. Keller Andover Kansas Police Department). https://www.justice.gov/ag/page/file/1272811/download

[5] https://www.eff.org/cyberspace-independence A Declaration of the Independence of Cyberspace The term digital native describes a person who has grown up in the digital age, rather than having acquired familiarity with digital systems as an adult, as a digital immigrant. Both terms were used as early as 1996 as part of the Declaration of the Independence of Cyberspace. They are often used to describe the digital gap in terms of the ability of technological use among people born from 1980 onward and those born before.

[6] https://www.govtech.com/public-safety/Report-As-Tech-Changes-Law-Enforcement-Its-Workforce-Must-Adapt.html

The National Institute of Justice (NIJ) provided funding to the RTI International (RTI) and the Police Executive Research Forum (PERF) to review the various technologies that law enforcement agencies were purchasing and using to augment their roles.[7] The results of the study were useful in providing guidance to law enforcement on key aspects to consider when implementing technology. The study found that out of the more than 1,200 state and local law enforcement agencies, 96 percent had adopted at least one of the 18 main technologies listed in the survey:

- seventy percent used in-car cameras
- sixty-eight percent used platforms that facilitate the transfer of information
- sixty-eight percent used social media

In addition, one-third of agencies used:

- body-worn cameras (BWCs)
- software to track cell phones
- geographic information system technology (GIS)
- software to investigate and manage cases

There was a pattern among larger agencies that had 250 or more officers to use technology that had analytical and visual features.

The results of the study indicated that law enforcement's use of technology was on the rise and would continue to increase in the future in both large agencies and smaller agencies. Predictive analytics software, BWCs, and next-generation 9-1-1 were among some of the technologies forecasted to increase in use.

Nationally, the study revealed that there was no significant correlation between the amount of technologies used by agencies and the policing strategies that they chose to use. In contrast, the number and type of technologies used by larger agencies varied based on the type of policing strategies that they implemented.

A crucial finding from the study was the indication that the technology acquisition process in many agencies was not always carried out in a methodical, planned manner. New technologies were often purchased and implemented on an "ad hoc" basis and were not tied to organized, strategic assessments.

The tendency to purchase technology without a clear, strategic plan can result in limited integration within the agency and a failure to recognize the primary or secondary benefits of the technology. These factors can lead to a lack of continuation funding for maintaining or updating particular types of technology.

[BEGIN TEXT BOX]

Using a Combination of Technologies to Catch a Triple Murderer

Sheriff Al Cannon, a state investigator in Charleston County, South Carolina, and Officer Ronald Maugan recounted the story of a modern homicide case that the collaboration of several police departments solved by using various technologies. The suspect had previously killed two elderly women which resulted in a "be on the lookout" order. He then murdered the clerk of a convenience store, where he stole the victim's phone and some lottery tickets. Surveillance cameras tipped officers off when he committed the crimes.

The suspect had also stolen a vehicle, and officers used an automated license plate reader to locate it. Law enforcement also contacted the cell phone provider, who pinged the stolen telephone and traced the cell phone. Using GPS coordinates, they tracked the suspect between two intersections in an adjoining county and figured out the direction he was headed.

[7] https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf

Investigators took the shell casings that were left at the scene and matched them to another set of shell casings, linking the suspect to an earlier homicide. When the suspect cashed in the winning lottery tickets that he had stolen, the officers identified his location using technology that tracks lottery tickets. In addition, video cameras at those locations captured the suspect's face.

Later, with the help of the National Integrated Ballistic Identification System, investigators matched bullet casings, which confirmed that the suspect taken into custody was actually the person who had killed the two elderly women. The United States Marshals' Fugitive Task Force tracked down and arrested the suspect He was later sentenced to life in prison.

[END TEXT BOX]

6.1.1 Law enforcement agencies should employ a consistent and comprehensive framework when considering the adoption of new technologies.

To assess the costs, benefits, and risks associated with adopting a new technology, law enforcement agencies should employ a consistent and comprehensive framework of analysis and approach to the issue. This framework should be general enough to apply to a broad range of technologies, yet specific enough to ensure agencies consider, at a minimum, the predictable significant costs and risks associated with the adoption of a particular technology. Not all elements of the framework may be needed to address each technology. Additionally, the framework must periodically be refreshed to ensure it accommodates newly identified risks or benefits posed from changes in mission or law, the emergence of other technologies, or public perception.

Agencies usually consider the adoption of a technology first, and then consider how to implement a particular technology efficiently within their organization. When law enforcement learns of a new technology, the operational benefits of deploying that technology may be immediately apparent. What is less apparent are the back-end risks or cost associated with deploying that technology. The change between the two assessments may depend on the technology at issue. Additionally, information obtained during the technology adoption phase may well inform the direction of the technology implementation phase.

Questions to ask during the technology adoption phase may include

- What is the purpose of adopting this technology?
- How will this technology advance my law enforcement mission?
- What are the initial and recurring financial costs associated with the technology?
- What are the legal, ethical, or policy implications of use of the technology and any data obtained via the technology?
- What are the potential implications on privacy and civil liberties?
- What might be the public's reaction?
- What additional risks could the agency be exposed to should they choose to adopt the new technology?

6.1.2 Law enforcement agencies should employ a consistent and comprehensive framework when considering the implementation of new technologies.

Similar to using a framework through which to assess the adoption of a new technology, law enforcement agencies should deploy a framework of analysis regarding the implementation of that technology. Some of the issues overlap with those addressed in the adoption phase. The implementation phase is when careful thought must be given to practical implications associated with providing the technology to and its use by law enforcement personnel in a legal, ethical and efficacious manner. Questions to ask during the implementation phase may include

- How will this technology be deployed and by whom?

- Who will have access to the technology or data obtained by it?
- How will use of the new technology be audited to ensure sensitive data is protected and public confidence is maintained?
- What training is required on the use of the technology or handling of the data, how often must it be conducted, and by whom?
- How will the officers' work routines change because of the new technology?
- What obligations might there be in adopting a particular technology on the larger agencies, that have the wherewithal to obtain these expensive technologies, to share these technologies with smaller neighboring agencies?

6.1.3 Law enforcement agencies should consider participating in regional partnerships or mutual aid agreements when considering the adoption of new technology which may be particularly expensive, manpower intensive, or not used frequently enough to justify sole ownership or operation by a single agency.

[CROSS REFERENCE GRANTS; RURAL AND TRIBAL; HOMELAND SECURITY]

Sheriff Al Cannon and Chief Robert Tracy both note that law enforcement agencies generally look favorably upon collaborative efforts when considering the adoption of a new technology and the corresponding need for grants to support its implementation.[89] After 9/11, the federal government made grants available to local, state, and tribal law enforcement to develop the necessary capabilities to identify and prevent future terrorist attacks. Unfortunately, there was not sufficient funding to provide the necessary resources to address all identified threat vulnerabilities.

Departments of all sizes can benefit from regional partnerships and mutual aid agreements, particularly when it comes to adopting new technologies which often bring an increased workload for personnel. One example of the success of this approach can be found in the mutual aid arrangements between law enforcement agencies in Delaware for unmanned aircraft systems (UAS) or drone technology. Consistent with these agreements, agencies with drones and pilots routinely respond to provide relief and support to partner agencies, in addition to agencies and jurisdictions that do not have the technology, and there is also a designated on-call pilot at all times for statewide needs. With this approach, agencies without the capacity to fund and administer a drone program by themselves can benefit from the technology through the support of their partners. This has made the use of drone technology by Delaware law enforcement more efficient and cost-effective.

Criminals have also become increasingly adept at using emerging technology to advance their schemes and activities. While law enforcement recognizes that new technology must be acquired to address criminal activity, the breadth of technology required may prove prohibitive for any one police agency to address. In many instances, medium-sized and smaller agencies may not be able to alone afford the purchase of a single technology because of a high total cost of purchase, which includes maintenance and sustainment costs as well as the need to hire and maintain a workforce savvy in one particular type of technology. At the same time, multiple technologies are required to operate in today's environment. And each of these technologies (e.g., facial recognition, automated license plate readers (ALPR), and biometrics) bring with them unique questions of law and policy that need to be addressed to ensure their use is done in a manner consistent with Constitutional and statutory constraints, particularly as it relates to privacy and civil liberties. A regional approach to technology acquisition allows agencies to share the cost and the expertise in specific areas.

[8] Al Cannon (Sheriff, Charleston County, SC, In discussion with Technology Working Group, Virtual Meeting, February 28, 2020.
[9] Robert Tracy (Chief, Wilmington, DE, Chief of Police, email Communication with Technology Working Group Federal Program Manager, Joe Heaps, March 24, 2020.

In some cases, agencies have pooled resources for shared or joint Computer Aided Dispatch/Record Management Systems (CAD/RMS). This allows agencies to share financial burdens and decreases the likelihood of interoperability challenges.

[BEGIN TEXT BOX]

Framework Considerations for the Use of ALPR Technology

Before implementing a new technology, it is imperative to understand the total cost of ownership as well as the full range of benefits. Automated license plate readers (ALPRs) are among the many technologies available for use by law enforcement. Sheriff Al Cannon Jr. from the Charleston County Sheriff's Office in South Carolina ran the ALPR technology through the framework as an example of some of the crucial elements to consider during the technology adoption process. ALPR is a system of cameras, supporting software, and server engines that capture license plate information along with the location, date, and time of the vehicle. The system instantly compares plate numbers to a database of wanted persons or criminals, AMBER Alerts, stolen vehicles, suspended license plates, individuals on terrorist watch lists, and other criminal activity. There are multiple benefits of this technology:

- Thousands of license plates are scanned in the same amount of time that it takes an actual person to scan one hundred.
- ALPR acts as a force multiplier for police departments in times when budgets and staffing are lean and uncertain.
- More suspect vehicles can be detected and arrests made, leading to increased safety for both civilians and police.
- The public's concerns regarding profiling can be alleviated because every vehicle is scanned regardless of who is driving.
- APLR helps identify vehicles connected with unpaid fines and helps cities collect unpaid revenue, such as outstanding citations or expired registrations.

Along with the benefits, law enforcement must also consider the potential drawbacks or special requirements of any new technology:

- Training
    - All users must obtain and maintain National Crime Information Center (NCIC) certification before operating the system.
    - Failure to maintain NCIC certification will result in the automatic suspension of access to the system until the certification is reacquired.
- Funding/Costs
    - State-funded portable units may be provided by request, but agencies should expect to increase their budget and/or seek grant funding as there is an exorbitant cost (minimum $15,000 just for fixed cameras) to implement this technology and ongoing costs to maintain the technology such as data storage or warranty coverage.
- Possible Public Reaction
    - Invasion of privacy
    - Fear of data being kept and retrieved indefinitely
- Data Challenges
    - Data entry must be timely and updated frequently.
- Technical Issues
    - Misreads on plates from different states
    - Obstruction of view or damage to system
    - False alerts on roadway signs

- Cameras not placed in ideal areas

[END TEXT BOX]

6.1.4 Law enforcement agencies should thoroughly research and consider the full range of policy, legal, Constitutional, and ethical implications, as well as privacy impacts associated with the adoption of any new technologies.

When law enforcement agencies determine that they will implement a specific technology, they must consider the legal implications of the use of the technology, including any affirmative authorizations required or constraints imposed as well as any impact on the privacy rights and civil liberties of their constituents. In addition to the widely discussed warrant requirements imposed by the Fourth Amendment to the Constitution as it relates to an individual's right to privacy and assessed by the courts, there may also be statutory limitations on the acquisition and use of various types of information that require a specified level of legal process. In the City of Ontario v. Quon (2010), a case involving an employer-provided text message capable pager, the U.S. Supreme Court decided the case on a very narrow question, explicitly refusing to consider the far-reaching issues raised on the grounds that modern technology and its role in society was still evolving. Although it is 10 years later, that statement still stands. In the interim, U.S. Supreme Court cases like U.S. v. Jones (involving tracking devices), and U.S. v. Carpenter (involving location information) provide insight to the court's assessment of the evolving nature of technology and its implications on constitutionally protected individual privacy interests.

Although applicable to only the states involved, state supreme court cases are also informative. In a recent supreme judicial court ruling, the highest court in Massachusetts concluded that, while "the defendant has a constitutionally protected expectation of privacy in the whole of his public movements," the manner in which law enforcement used data obtained from APLRs in this particular case did not violate his constitutional rights. Law enforcement agencies should be mindful of these court decisions and the impact any new technology may have on constitutionally protected privacy interests. Likewise, law enforcement agencies should consider statutory limitations and authorizations that may affect the deployment of a specific technology.

6.1.5 Law enforcement should engage all impacted constituencies, such as members of the community and other law enforcement agencies, when considering the adoption of a new technology.

Groups who may be affected by the implementation of a new technology include the general public, elected officials, local advocacy groups, and law enforcement labor organizations. In addition, non-traditional partners such as the American Civil Liberties Association (ACLU), are increasingly willing to provide input, which can enhance public acceptance of law enforcement's use of a specific technology. As noted by Chief Roxanna Kennedy, Chula Vista Police Department (CVPD), the department successfully implemented a drone program based in part on the efforts by the department to engage the public and establish a cooperative environment in the community.[10] As noted by Chief Kennedy, the "Drone as a First Responder" program was effective because the police department proactively reached out to the community entering into a dialogue regarding the need for the program specifically as it pertained to the local community. The police department also remained transparent and fostered political support before implementing the program. By identifying and engaging the necessary stakeholders, the CVPD was able to obtain the approval and buy-in from members of the community who would be impacted by the program.[11]

---

[10] Roxana Kennedy (Chief, Chula Vista (CA) Police Department), in discussion with the Technology Group, April 22, 2020.

[11] Roxana Kennedy (Chief, Chula Vista (CA) Police Department), in discussion with the Technology Group, April 22, 2020.

The Wilmington, Delaware, police department had a similarly favorable experience when pioneering their use of UAS technology in 2014.[12] The department effectively communicated the use and benefits of the technology for law enforcement and public safety to obtain buy-in from the public and government officials. The department started with limited equipment; over time, their UAS program has grown, and they have acquired additional equipment and discovered new ways to leverage the technology.

[BEGIN TEXT BOX]

Bird's Eye View: Averting Potential Crisis by Using Unmanned Aircraft Systems (UAS) Technology

On August 24, 2017, around 10 p.m., one of our police officers was working alongside an agent with Delaware Probation and Parole in the 1700 block of Tulip Street in Wilmington when gunshots were fired in their direction. As you can imagine, the incident drew a significant law enforcement response, including police officers from our department and surrounding jurisdictions along with tactical teams. The search for the gunman led officers to an alley that was fenced in and largely obscured from view, and officers heard sounds coming from the alleyway. Given the late hour and lack of visibility, a tactical team breaching the alleyway would have certainly put officers at risk should the suspect have been present, and so our team deployed a drone equipped with an on-board thermal imaging camera. The drone was able to show us that the movement was coming from a dog that was in the alley – and not an armed gunman. The use of a drone in that situation helped to ensure that our officers were not put into harm's way attempting to clear the alley in the middle of the night, and could have possibly prevented officers being surprised by the dog and potentially discharging their weapons. It gave us the situational awareness we needed, without a single person being at risk. - Chief Robert Tracy, Chief of the Wilmington Delaware Police Department

[END TEXT BOX]

6.1.6 Law enforcement agencies should assess the overall impact to the agency and its personnel prior to adopting a new technology (e.g., individual officer workload and other aggregate agency stressors).

In addition to assessing how the use of the new technology may affect external constituencies, law enforcement agencies should also consider the impact the use of such technology would have on its own personnel and agency resources. Fundamental questions of how the technology helps officers interact with the public or how it may allow law enforcement to better use its resources may lead to unanticipated benefits to include de-escalation of events or quicker response times. As evidenced by the CVPD experience with UAS, introduction of the technology directly supported the officers' ability to de-escalate otherwise difficult response efforts. By sending the UAS in to observe the scene prior to their arrival, law enforcement was able to gain insight as to what was actually happening on the ground. This advanced intelligence information allowed law enforcement to better assess their needs and prepare to respond in a manner that let them allocate resources more effectively. CVPD also uses drones to respond to 9-1-1 calls in a program called Drone as a First Responder.[13] CVPD works closely with the Federal Aviation Administration (FAA) as part of the FAA UAS Integration Pilot Program (IPP).[14] Within the UAS range, the UAS response time is under three minutes and ground units arrive ahead of the UAS just over half the

[12] Adam Ringle (Sergeant, head of the Forensic Services Unit, Wilmington, (DE) Police Department), in discussion with the Technology Group, April 22, 2020.

[13] Sallee, Verne. Captain, Patrol Operations, Chula Vista Police Department, California "Drone as a First Responder THE NEW PARADIGM IN PUBLIC SAFETY." Police Chief Magazine March 2020,
[14] https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=23574

time. During a recent period, CVPD indicates the UAS teleoperators[15] were able to clear more than 15 percent of calls without requiring ground unit response.[16]

Conversely, a well-intended but unnecessarily complex data entry system can actually lead to less productivity and an increase in officer frustration. It's often the second or even third level of cascading consequences that are the most difficult to predict. Agencies should consider trial-periods with new technology and seek to gather experiences from other agencies who have deployed the same or similar systems.

6.1.7 **Law enforcement agencies should thoroughly research potential vendors, products, and services to ensure the greatest efficacy, security, and reliability. Where applicable and appropriate, law enforcement agencies should consider adherence to professional standards and accreditation programs when selecting products and services.**

Emerging technologies are entering the market place at a rapid rate with which it is often difficult to keep pace. Despite this reality, it is incumbent upon law enforcement agencies to understand the vendors they are dealing with as well as the products and services they are considering adopting or acquiring. In the current market, issues such as how long the vendor has been in business and the likelihood it will continue to be in business may be valid areas to assess. As with any procurement, law enforcement agencies should endeavor to determine whether the capabilities presented by the vendor are accurate and whether the vendor's performance and assertions can be validated. Due to the sensitive nature of law enforcement activities, the privacy rights and civil liberties implicated by those activities, special consideration should be paid when assessing non-domestic (i.e., foreign) vendors for both supply chain and security reasons.

As an independent arbiter of a vendor's products, agencies should identify and understand any relevant industry standards that apply to the technology at issue. This will allow agencies to determine whether the technology has any specific limitations as well as whether the technology is compatible with the current systems. Similarly, use of state purchasing contracts or similar vehicles may prove helpful in surfacing prior efforts to vet vendors and could lead to time and cost savings. [17] Agencies must take care not to attempt to employ technology in ways it was not intended or for which it is not yet mature enough to be used. The evolution of Rapid DNA technology, for example, illustrates how technology designed for the rapid analysis of DNA, taken from a single source, could be erroneously used to try and analyze DNA from a much less discreet source, which may lead to substantial efficacy issues. Rapid DNA was originally envisioned as a fully automated process of developing a DNA profile without human intervention from a cheek swab (taken from a single human). Over the last few years, interest has grown in using Rapid DNA technology to quickly analyze evidence gathered from crime scenes. While Rapid DNA may be able to develop a DNA profile quickly, at present, Rapid DNA instruments and collection protocols are not sufficiently mature for use in analyzing crime scene evidence.

In exercising due diligence researching such systems, agencies would likely find

- Rapid instruments are not as sensitive as conventional forensic laboratory techniques and require significantly more samples to obtain a DNA profile.

---

[15] Teleoperator is a sworn police officer and a drone operator who listens to 911 calls live and is able to launch the drone based upon what they hear. CVPD is the first police department in the nation to test and use Live911 (Live911.com). Using the information from the live 911 call, and in partnership with HigherGround www.higherground.com, CVPD allows the teleoperator, and soon officers in the field, to listen live to ongoing 911 calls. The Live911 App is being installed in patrol vehicles. https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program .

[16] Sallee, Verne. Captain, Patrol Operations, Chula Vista Police Department, California "Drone as a First Responder THE NEW PARADIGM IN PUBLIC SAFETY." Police Chief Magazine March 2020,

[17] Al Cannon, Sheriff, Charlestown County, South Carolina, In discussion with Technology Working Group Federal Program Manager, Joe Heaps, February 28, 2020.

- Crime scene samples may be mixtures and contain low quantity or degraded DNA, which may require interpretation from a qualified DNA analyst.
- Rapid DNA instruments are currently unable to meet certain aspects of the Federal Bureau of Investigation's (FBI) *Quality Assurance Standards for Forensic DNA Testing Laboratories*.
- No approved expert systems for crime scene samples exist that allow a DNA profile to be generated without interpretation from a qualified analyst.
- To obtain optimal results from a Rapid DNA instrument, uses of the system require specialized training and experience in assessing crime scene evidence and determining what type of testing is appropriate.

[CROSS-REFERENCE RECRUITMENT, RETENTION, AND TRAINING]

Law enforcement agencies must thoroughly assess these types of issues to ensure that they accurately weigh the limitations of the proposed technology as well as any limitations of the vendor's ability to provide the necessary technological components.

6.1.8 Law enforcement agencies should understand and account for the total cost of ownership as well as the full range of benefits when considering the operation of the new technology.

The total costs of ownership of new technology include not only the upfront costs associated with acquiring the technology but also the costs of operating and maintaining the technology. Consideration must be given to the use, storage and maintenance of the technological systems as well as any data they generate. Additional costs may include those associated with training, certification, intellectual property licenses, or online access fees.

An example of a relatively emerging technology which may have unanticipated benefits is acoustic detection technology. Specifically, gunshot detection technology has provided law enforcement agencies, particularly those in urban settings, with a significant tool to combat firearm crime and violence. In addition to the significant investigative and evidentiary gains that can result from the implementation of this technology, a crucial outcome is that police are made aware of nearly every firearm discharge. Much like a car accident that motorists pass by without reporting, assuming someone else has alerted first responders, there remains a lapse in reporting gunfire, particularly when no one is struck; a 2016 Brookings Institute study reported that more than 80 percent of gunfire goes unreported to police.[18] The result is a lack of awareness of shots fired incidents—which are often failed shootings likely to be attempted again—by police, and a growing sense in the community that assumes police are notified but do not care enough to respond.

Gunshot detection technology helps to remedy these issues, and when coupled with cutting-edge investigative techniques like National Integrated Ballistic Information Network (NIBIN) tracing and analysis, can have a significant effect on gun crime. Wilmington Police Department has a partnership with the Bureau of Alcohol, Tobacco, Firearms and Explosives, and an embedded Crime Gun Intelligence Center, with rapid collection, tracing and analysis of recovered shell casings and firearms. This generates real-time intelligence that can be disseminated to detectives and patrol officers, and has been a key component in bringing about historic reductions in gun violence. Wilmington Police Department is also represented on the National Crime Gun Intelligence Governing Board with the ATF, which works to further develop and expand integration of these components of violence reduction throughout the country. Acoustic detection technology uses sensors to determine gunfire and allows analysts to pinpoint the location and immediately provide that information to police. This technology had the unanticipated benefit of allowing officers to decrease their response time to complaints and incidents.

[18] Carr, Jillian and Doleac, Jennifer L., The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data (April 26, 2016). Available at SSRN: https://ssrn.com/abstract=2770506 or http://dx.doi.org/10.2139/ssrn.2770506

Most acoustic detection technology systems range in cost from $40,000 to $60,000 per square mile for high-crime areas, and these costs must be paid each year in addition to any initial set up costs.

[CROSS REFERENCE REDUCTION IN CRIME]

6.1.9 **Law enforcement agencies should apply cybersecurity frameworks when implementing technologies underpinned by digital or cyber components.**

Modern law enforcement agencies work in a highly complex, interconnected environment. The technology that law enforcement agencies use and the sensitive data they access and generate suggests they require strong cyber security risk frameworks. Agencies must diligently employ and routinely audit those cyber risk mitigation strategies developed through the frameworks' use to ensure effective implementation and actual risk reduction.

6.2 Creating and Using New Data Capabilities

Background

As part of the process for deploying new technology that will generate or acquire new data sets for law enforcement use, law enforcement agencies should describe how they will use the data generated or acquired by the new technology and the goals they are trying to achieve. It can be difficult for law enforcement agencies to deploy technology that generates or acquires data with a full understanding of the spectrum of associated costs and risks, or the broad range of data management requirements that may accompany the new dataset obtained. Using a framework to determine costs and risks of generating, acquiring or using new data can ensure agencies ask the right questions and thoroughly consider relevant issues Similar to the recommended technology framework, the data framework must be general enough to be applicable across a broad range of data types, yet specific enough to ensure agencies consider, at a minimum, the basic, predictable costs, benefits, risks, and any new obligations associated with the development of a new data enabled capability. The framework should be comprehensive to accommodate key questions, regardless if the new data set is to be generated anew internal to the law enforcement organization, acquired externally from commercial or other partners, or created through the aggregation of different internal or external datasets. The framework may even help the agency ensure that they consider data interoperability questions which may have significant impacts on their ability to fully use the data in the future. Agencies should also routinely refresh and reengage their framework to accommodate changes in technology, mission, law, or even changes in public perception.

Current State of the Issue

The internet and rapid advancement of technology has given rise to a digital explosion of data. In the commercial communications industry alone, personal mobile devices generate and platforms routinely collect enormous amounts of data for marketing and other product development purposes. Law enforcement agencies are likewise, albeit to a lesser magnitude, generating and accumulating rapidly increasing amounts of data internal to their own organizations. Often this data is generated without agencies even thinking about the myriad of attendant issues. For example, police vehicles now routinely report location and maintenance information to the owning departments, and in-car computers are constantly generating usage and other metadata while simultaneously receiving input via the keyboard. Operational and investigative technologies such as license plate readers and body worn cameras are also creating large data sets. Yet, agencies may still fail to appreciate the full range of costs, benefits, and risks associated with the deployment of the new technology and the intentional generation and acquisition of the related data. The generation or acquisition of these new data sets not only come with risks, costs and benefits, they also bring with them new obligations to protect and ensure the appropriate use of data. Additionally, new and sophisticated data aggregation and analysis techniques (e.g., artificial intelligence) may also add new value to data that law enforcement did not anticipate when it was first collected. In the case of the Golden State Killer, for instance, law enforcement effectively leveraged DNA data collected for commercial purposes to trace people's ancestry to identify a suspect in a cold case.

6.2.1 **Law enforcement agencies should endeavor to thoroughly consider the full range of potential legal,**

constitutional, civil liberties and privacy implications associated with the generation, acquisition or use of any new data set.

Within the last few years, the volume of third party data available for resale to public and private entities has grown exponentially. Certain commercially available data may hold great value for federal, state, and local law enforcement. However, data being shared publicly or by and between commercial entities may take on additional sensitivities when obtained or accessed by law enforcement. Commercial entities may restrict law enforcement access to or use of commercial data. Also, constitutional, statutory, or legal restrictions may apply when that data is obtained by law enforcement for investigative purposes. In addition to considering commercial restrictions on use, privacy and civil liberties concerns are frequently implicated by how data is stored and managed. As such, law enforcement agencies will need to consider data use safeguards, auditing, and strong data protection regimes for each data set generated or acquired.

6.2.2 Law enforcement agencies should communicate transparently with the community to ensure a clear understanding regarding new datasets, how they are being used, and what protections are in place to ensure their appropriate use and protection.

Public trust in law enforcement's actions is vital to effective policing. Agencies should determine if the public will generally support or object to law enforcement's use of a particular dataset for a particular law enforcement purpose (e.g., public expectations of the propriety nature of the data, safety, privacy, and protection of civil liberties as implicated with use of the data for law enforcement or public safety purposes). Additionally, agencies must consider how courts and juries may view law enforcement's use of any new dataset. This effort may be aided by the Executive Office for United States Attorneys (EOUSA), the National District Attorneys Association (NDAA), or the legal section of International Association of Chiefs of Police (IACP), to name a few. Law enforcement should also determine if there are any accreditation regimes associated with the storage or management of a new dataset, if they can withstand legal scrutiny, or if there are any legal implications by not using such regimes.

According to Jake Laperruque, Senior Counsel for The Constitution Project at the Project on Government Oversight (POGO), global positioning systems, drones, gunshot technology, APLRs, and facial recognition surveillance should be subject to checks and limitations. Law enforcement must continue to engage in effective, ethical, and accountable safeguards when using technology.

To further the public's understanding and perception of law enforcement's use of new datasets, agencies should consider the full range of communications platforms and avenues available to ensure awareness within the communities they serve. Law enforcement agencies should be as forthright as possible with regard to informing the public about law enforcements use of new data sets to include addressing data management and protection regimes and privacy and civil liberties concerns.

6.2.3 Law enforcement agencies should have a process to routinely evaluate data viability (e.g. degradation over time) and a process to determine when to stop using data, as well as how to securely archive or destroy data that are no longer needed or reliable.

Regardless of the origin of the data, law enforcement agencies must carefully consider how they will routinely evaluate the viability and reliability of data. Data efficacy often degrades over time. Agencies should consider how they will determine when a dataset needs to be refreshed, reconditioned, or no longer used and how it will ensure the appropriate destruction of data (e.g., retention and destruction schedules). Agencies should carefully consider the use of various storage media. The storage medium must accommodate the necessary requirements regarding security, capacity, and access speed as well as longevity. Law enforcement agencies will also have to consider if cloud storage solutions are a viable option.

6.2.4 Law enforcement agencies should carefully consider appropriate data formats for storage.

The format in which data is stored may have great implications for how that data is used and leveraged, now and in the future. As new data analytics technologies continue to evolve, highly proprietary or otherwise unique in-house storage arrangements may limit the ongoing or future use of a dataset.

Agencies should carefully consider what data reporting requirements might be met, enabled, or precluded through the use of a particular data format. Similarly, data sharing among law enforcement agencies can have enormous investigative and officer safety benefits, only if the data is stored in such a way that it can be made easily accessible by other systems in a manner consistent with all relevant safeguards and protections. Conversely, in some cases particular data structures and schemas may be intentionally employed to ensure data cannot be read by other systems, or aggregated with other datasets in an effort to enhance security, privacy, or better protect civil liberties.

[CROSS REFERENCE OFFICER HEALTH AND WELLNESS]

6.2.5 Law enforcement agencies should determine and account for the total cost of ownership of the data capability.

When developing or acquiring a data enabled capability, some law enforcement agencies find it difficult to factor in the total ownership cost or "life cycle" cost of the capability. This total cost includes all costs associated with procurement, implementation, ongoing fees, maintenance, and recapitalization required to support the data-enabled capability requirements. Frequently, agencies budget for the upfront costs associated with the development of the data capability but do not adequately assess and plan for the additional, and usually growing, recurring costs of maintaining and refreshing systems. Maintenance costs include costs for storage, extraction and migration, additional infrastructure, and bandwidth. Refresh costs are those required to recapitalize a system to meet storage, security, and performance requirements.

As technology and data capabilities continually improve and evolve, so does the requirement to ensure systems and datasets are upgraded or replaced. As a result, some law enforcement agencies have shifted data capabilities to the cloud, transferring many of these lifecycle costs into more negotiated, up-front, or predictable costs. Finally, law enforcement agencies should exercise caution when initially funding the development of new data capabilities, particularly when done with one-time funding. If an agency decides to use one-year grant money to develop or acquire a data capability, it must identify a secondary funding source to address total ownership costs before moving forward.

[CROSS REFERENCE GRANTS]

6.2.6 Law enforcement agencies should determine and account for the cybersecurity implications of the new dataset.

It is imperative for law enforcement agencies to appropriately secure their data. To that end, agencies should identify a cybersecurity framework to follow such as the National Institute of Standards and Technology (NIST)[19] guidelines or the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000 series (ISO/IEC 27000)[20] of information security standards. The use of standards in implementing cyber security should be strongly encouraged by all law enforcement professionals. Additionally, agencies should develop and exercise a data exposure response plan to mitigate the impact of data breaches that may result from a host of threats such as insider threats, hacking, or spillage.

[19] https://www.nist.gov/tpo/department-commerce
[20] https://www.iso.org/isoiec-27001-information-security.html

6.3 Lawful Access

PULL QUOTE: "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."[21] - Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation

Background

Law enforcement's ability to access electronic evidence has slowly eroded over the last decade. A growing number of US tech companies have or are promising to transition from managed strong encryption[22] models to user-access-only and end-to-end encryption models which, by design, preclude court authorized lawful access to evidence.[23] If the end user is a criminal or terrorist, these products and services may help them hide or immunize dangerous illegal conduct. Because of warrant-proof encryption, agencies often cannot obtain the electronic evidence and intelligence necessary to investigate and prosecute threats to public safety and national security, even with a Constitutionally-valid warrant or court order. This creates a "lawless space" that criminals, terrorists, spies, and other bad actors can exploit.

Current State of the Issue

PULL QUOTE: "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."[24] - Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation

As more companies transition from managed strong encryption models to user-access-only and end-to-end encryption models, the net effect is the barring of lawful access to otherwise accessible, court authorized information. While many of the most widely known instances of this challenge publicized by

---

[21] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Issues and Problems that Technology Presents to Law Enforcement in Crime Reduction Lawful Access and Dark Web, Part 1, Before the Commission (April 15, 2020) (written statement of Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation). https://www.justice.gov/ag/page/file/1272811/download

[22] The primary definition of the common usage of the term "encryption" is "the act or process of encrypting something: a conversion of something (such as data) into a code or cipher." See Miriam-Webster on-line American Dictionary at: https://www.merriam-webster.com/dictionary/encryption.

[23] During the Technology Working Group's proceedings, a major on-line video-conferencing provider, made popular by the pandemic, Zoom, announced a change in its security policies. On April 1, 2020, Zoom issued a public statement describing how they utilize server to server encryption to maintain security for customers but felt the necessity of stating: "Zoom has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list." See https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/. Remarkably, on May 7, 2020, Zoom went further and issued another, yet stronger, facially anti-law enforcement public statement following their acquisition of Keybase announcing their intent to deploy end-to-end encryption. At that time, Zoom added in that blog entry the following statement: "Zoom has not and will not build a mechanism to decrypt live meetings for lawful intercept purposes. (Emphasis added.)" See https://blog.zoom.us/wordpress/2020/05/07/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering/.

[24] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Issues and Problems that Technology Presents to Law Enforcement in Crime Reduction Lawful Access and Dark Web, Part 1, Before the Commission (April 15, 2020) (written statement of Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation). https://www.justice.gov/ag/page/file/1272811/download

the media relate to the FBI and terrorism, the ubiquity of end-to-end encryption, and other user-only access encryption products and applications causes them to also be encountered daily by state and local police departments. The resultant impact means not only an increase in unsolvable crimes and a denial of justice for victims, but also threatens to dramatically affect the nation's dual-sovereign federal system of law enforcement. 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 whose own such resources are already taxed. In such a paradigm, the result may be that a federal decision on the application of such resources to a specific case may practicably dictate which state and local crimes are investigated and prosecuted regardless of the priorities of state and local officials.

In March of 2019, Facebook announced its intention to encrypt Facebook Messenger.[25] Reporting over 15 million CyberTipline reports a year, Facebook provides more reports to the National Center for Missing and Exploited Children (NCMEC) than any other tech company. While the commission recognizes and applauds Facebook's substantial efforts in combatting these heinous crimes against children, it is discouraging that Facebook may alter their systems in such a way as to all but cease providing this vital, actionable intelligence to NCMEC.

[BEGIN TEXT BOX]

"To date, NCMEC has received over 71 million CyberTipline reports, and the volume of content reported to the CyberTipline continues to rise each year. In 2018, NCMEC received over 18 million reports containing 45 million suspected child sexual exploitation images, videos, and related content. In 2019, NCMEC received slightly fewer reports—just under 17 million—but these reports contained over 69 million images, videos, and related content. Today the CyberTipline is a key tool in helping ESPs; members of the public; federal, state, and local law enforcement; and prosecutors combat online child sexual exploitation.[27]

[END TEXT BOX]

Historically, law enforcement has typically relied upon industry to provide technical assistance in identifying and transferring to officials specific information which meets the four corners of a predicated, constitutionally sound search warrant or order issued by a neutral and detached judge. The practice is usually the most efficient means of execution and preserves the privacy of information of others who are not the subject of the search warrant by ensuring that there is seldom any need or justification for law enforcement to physically or electronically enter a business system to search for the information themselves. Moreover, the practice creates a level enforcement playing field for the enforcement of state and local crimes with that of federal crimes because, unlike large federal agencies, state and local law enforcement agencies are frequently less likely to have the technological expertise to execute the order without such assistance.

In continuation of this practical, collaborative, privacy-enhancing practice, the New York district attorney's office reported to the commission about their efforts to resolve the technical assistance impasse with industry when they met with senior staff from Google and Apple in February 2020 to discuss potential ways for law enforcement to lawfully access mobile devices and technology used by criminals.[28] For many

[25] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

[26] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Juvenile Justice and Youth Crime Commission Hearing, Before the Commissioners (May 4, 2020) (written statement of John Clark, President & CEO, the National Center for Missing & Exploited Children).

[27] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Juvenile Justice and Youth Crime Commission Hearing, Before the Commissioners (May 4, 2020) (written statement of John Clark, President & CEO, the National Center for Missing & Exploited Children).

[28] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Issues and Problems that Technology Presents to Law Enforcement in Crime Reduction Lawful Access and Dark Web, Part 1, Before the Commission (April 15, 2020) (statement of Cyrus R. Vance Jr., District Attorney, New York County, New York). https://www.justice.gov/ag/page/file/1270036/download

years previous, Apple and Google routinely facilitated law enforcement's lawful access to their mobile phones or phones using their operating systems when the companies received a court-ordered search warrant. That changed in 2015 when Apple first rolled out an iOS mobile operating systems designed to make the content of its smart phones completely inaccessible by anyone except the user. Soon, other providers began following suit. In doing so, these companies have upended more than 200 years of jurisprudence by effectively placing otherwise accessible evidence beyond the reach of a court-ordered search warrant. In so doing, they have weakened the arm of justice and handicapped the constitutionally-enshrined, dual-sovereign paradigm for the fair and timely enforcement of all laws for the protection and promotion of the public's safety.

6.3.1 Congress should enact federal legislation 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.

PULL QUOTE: "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."[29] - Cyrus R. Vance Jr., New York District Attorney

The Communications Assistance for Law Enforcement Act (CALEA)[30] has not kept pace with the realities of today's modern internet and the near abandonment of the traditional telephone network by the public. In today's social media, always-on, always available, communications reality, app providers have not merely replaced a portion of the local telephone exchange, they have effectively become the local telephone exchange. Yet many such providers bear no social or legal responsibility to compensate for or mitigate the harms caused by criminal elements which they know routinely use their services and products with an impunity facilitated by their designs. Despite decades of candid discussions initiated by law enforcement with many of these providers and manufacturers, little progress has been made to resolve these issues voluntarily. Instead, during that period, the problem has only grown worse and now threatens to become the norm. Impenetrable encryption barring law enforcement's lawful access to evidence is rapidly extinguishing law enforcement's ability to protect the public.

Victims' rights are a major aspect of the lawful access issue. Today, victims bear much of the cost associated with online crime. Technology companies must accept more responsibility, either by doing more to prevent online crime or to begin paying more of the costs associated with their inaction. While tools like artificial intelligence (AI) offer some promise to help detect and prevent a portion of online crime, a lack of actionable evidence may still leave law enforcement unable to act and victims without justice.

In evaluating the call for legislation and the Constitutional duty of law enforcement to both respect and protect privacy, the commission considered yet rejected the idea that lawful access is the equivalent of a "back door." Almost all mobile device manufacturers, operating system vendors, and app providers maintain their own upgrade back doors which enables providers to routinely change almost all functions and settings of a device or service at will. Police access to content pursuant to a probable cause court order, which is ultimately subject to review and appeal, does not equate to a security risk. The commission recognizes that major financial institutions both in this country and abroad daily engage in billions of dollars-worth of transactions, and the security of these transactions is maintained and managed through strong encryption, yet such institutions also maintain the ability to access such information when justified and necessary. This duality suggests that the issue is not one of technological impossibility, but a question of willingness on the part of industry. The commission recognizes and

---

[29] President's Commission on Law Enforcement and the Administration of Justice: Hearings on Issues and Problems that Technology Presents to Law Enforcement in Crime Reduction Lawful Access and Dark Web, Part 1, Before the Commission (April 15, 2020) (written statement of Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation).
https://www.justice.gov/ag/page/file/1272811/download

[30] 47 U.S.C. §1001 *et seq.*

concurs with the December 2019 resolution of the IACP calling for world-wide legislation compelling companies to develop for themselves and implement appropriate lawful access capabilities for their products and services.[31]

The commission concludes that the impact and magnitude of the lawful access challenge 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 in corporate boardrooms, but should be returned to the representatives.

6.3.2 Congress should enact federal legislation that would grant civil liability immunity to technology companies for harms they caused or exacerbated be amended and conditioned upon such companies implementing effective mitigation strategies that include, at a minimum, creating and maintaining a lawful access capability.

Recent Congressional hearings have also cast light upon the effect that certain civil liability immunity statutes, adopted during the infancy of many high tech companies, may inadvertently be having in encouraging companies to aggressively pursue and market impenetrable encryption schemes. Some argue that, in the absence of any risk of financial liability for harms to victims caused or exacerbated by their products or services, some of statutorily-immune, high tech companies may not be influenced by the routine cost–benefit analysis most companies employ in determining whether to dedicate resources to harm-mitigation strategies, including facilitating lawful access. Consequently, so long as liability is impossible, the commission is left with the logical conclusion that any expense of maintaining lawful access capabilities could be seen by some companies as nothing more than an unnecessary drain on profits. Ultimately, impenetrable encryption in such an environment arguably removes the only remaining corporate risk—public outrage—by enabling plausible corporate ignorance of illegal uses and resulting harms and disingenuously cloaking corporate financial motivations under the public relations veil of a desire to enhance privacy. If corporations are to continue to enjoy liability immunity for harms caused or exacerbated by their products or services, particularly as they apply to the application of intractable encryption, they should be mandated to develop and maintain a lawful access solution capable of producing cleartext data in response to lawful court orders.

6.4 Lawful Access Technology Resource Center

Background

A significant shift in the technology–development paradigm in recent decades which has exacerbated the lawful access challenges for law enforcement was discussed and illustrated during the commission's proceedings. During the April 21, 2020, Reduction of Crime hearing, Commissioner Erica MacDonald posed a question to Dr. Richard Vorder Bruegge, a Senior Physical Scientist at the FBI, regarding the notion that "when it comes to technology and advancing technology, the government doctors [and] the government lawyers seem to always be playing catch up . . . is there something that we could do to be more proactive?" In response, Dr. Vorder Bruegge stated that "the last 50 years have seen an incredible transfer in the development of high technology from government-driven developments to private sector developments. So whereas 50 years ago, [the] Department of Defense or the federal government may have been driving technological innovation, now in the twenty-first century, we're seeing where it's the private sector doing that." Dr. Vorder Bruegge later expanded upon his initial response by identifying two key areas of consideration during the technology acquisition process: "Will the requirement owner be able to iterate this tool for changed purposes/requirements in the future?" and "How is this tool going to be interoperable with other tools (e.g., one shared user inter-face for a radar, vice a camera, vice an RF-based technology, so that a control center or operations center watch officer can look at one thing or one

[31] See IACP December 2019 Resolution: "Worldwide Call for Legislation and/or Appropriate Regulation That Mandates Encryption Implementation Regimes That Maintain Reasonable Security of Communications and Stored Data, yet Permit Lawful Access by Law Enforcement Pursuant to the Rule of Law" at page 45 at https://www.theiacp.org/sites/default/files/Adopted%202019%20Resolutions__Final.pdf.

group of things rather than [three to four] different user interfaces)."[32][33]

[CROSS REFERENCE REDUCTION IN CRIME; HOMELAND SECURITY]

That the pace of both the evolution and iteration of technologies that hold potential to assist and challenge society's law enforcement mission has become frenzied is an axiomatic fact of modern life and need not be detailed further here. In this context, however, reason and common experience demonstrate that few police departments possess the resources to keep abreast of this evolution on an ongoing basis. The need for an enduring, shared, collaborative structure that can serve as a hub for technical knowledge management, facilitate the sharing of solutions and know-how among law enforcement agencies, and inform and strengthen law enforcement's relationships with the communication industry is self-evident.

Current State of the Issue

One asset already assisting federal, state, and local agencies to keep abreast of the communications revolution has been the National Domestic Communications Assistance Center (NDCAC). Located in Fredericksburg, Virginia, the NDCAC is a core FBI-sponsored technology group composed of engineering personnel and contractors who work collaboratively with fellow federal, state, and local law enforcement officers who possess technical training or aptitude and who are assigned to or associated with the NDCAC. The NDCAC also has access to and collaborates with engineers and technical staff of the FBI's Operational Technology Division (OTD) which is charged with effectuating court-ordered wiretaps and the forensic search of stored electronic information. Thus, to a limited extent, the NDCAC already serves as a hub for technical knowledge management that facilitates the sharing of solutions and know-how among law enforcement agencies, and informs and strengthens law enforcement's relationships with the communication industry. However, as structured today, the NDCAC focuses almost exclusively on issues involving real-time lawful interception and the recovery of stored communications. NDCAC engineers are involved in the testing of industry-developed lawful intercept technical solutions that purport to comply with the CALEA,[34] and they provide substantive technical input and closely monitor the work of industry standards settings groups as it relates to lawful access issues. The NDCAC also operates a nationwide assistance call center available to verified law enforcement officers engaged in criminal investigations involving many of the nation's most tragic and serious crimes.[35] In addition, the NDCAC also offers, funding permitting, periodic technology and digital forensic training sessions to state and local officers. Unfortunately, the NDCAC's current mission and resources are inadequate to fully confront, track, assess, and generate recommendations to redress the rapidly evolving challenges of modern technologies on a larger scale.

6.4.1 The Federal Bureau of Investigation should restructure the NDCAC Executive Advisory Board to ensure an environment wherein law enforcement executives from federal, state and local agencies may

---

[32] President's Commission on Law Enforcement and the Administration of Justice: Reduction of Crime Hearing Technology Tools Panel, Before the Commission (April 21, 2020) (statement of Erica MacDonald, Commissioner). https://www.justice.gov/ag/page/file/1272811/download

[33] President's Commission on Law Enforcement and the Administration of Justice: Reduction of Crime Hearing Technology Tools Panel, Before the Commission (April 21, 2020) (statement of Dr. Richard Vorder Bruegge, Senior Physical Scientist, Federal Bureau of Investigation). https://www.justice.gov/ag/page/file/1272811/download

[34] CALEA, 47 U.S.C. §1001 *et seq.* requires, in essence, that a defined class of "telecommunications carriers" develop for themselves and their services lawful interception solutions which they alone control but which may be activated by the carriers where and when they are presented with a lawful order, such as court wiretap order issued after a finding of probable cause by a neutral and detached judge. CALEA has historically applied primarily to traditional telecommunications companies operating land-line, cellular/mobile and cable-based telephony. CALEA has not yet been found to explicitly apply to so-called "over-the-top" software-only-based application providers whose services generally do not manage communications connecting to the public-switched telephone network but which have all but totally replaced and supplanted the local telephone exchanges.

[35] The NDCAC's Law Enforcement Assistance line managed by the Technology Resources Group is 1.855.306.3222.

address specific and sensitive law enforcement matters including the impact and development of emerging technology on law enforcement operations.

Currently the NDCAC is assisted in its mission through the use of an Executive Advisory Board (EAB) which is composed of approximately fifteen members representing a wide range of federal, state, and local law enforcement agencies. The EAB process has reportedly evolved to provide some measure of state and local insight to inform the vision of the NDCAC, but it has limitations. The current structure of the EAB reportedly presents structural and procedural limitations for law enforcement to candidly and confidently share and discuss in a public setting sensitive operational information relating to on-going investigations that involve technology requirements and objectives as well as gaps, limitations, and vulnerabilities.

Restructuring of the EAB board in a manner that would encourage and ensure an environment exists wherein law enforcement executives may freely collaborate would be a necessary first step in creating a mechanism through which law enforcement may collaborate over their shared needs. Consultation and voluntary collaboration with industry cannot occur unless all law enforcement agencies—large, small, urban and rural—have a means of gaining not merely a basic understanding of emerging technologies, but an informed ability to identify and prioritize their evolving operational and managerial technology impacts, challenges, opportunities, gaps, and requirements.

6.4.2 The National Domestic Communications Assistance Center Executive Advisory Board should develop technology review analytical frameworks through which the NDCAC and law enforcement agencies may uniformly identify and evaluate issues in advance of emerging technology adoption, generated by classes of technologies.

The mission of the NDCAC and the role of participating law enforcement agencies should be expanded to reflect the increased need of the federal, state, and local law enforcement community to address challenges of emerging technologies. The expanded mission will ensure the NDCAC can uniformly identify and evaluate, in advance of emerging technology adoption, issues generated by classes of technologies such as, but not limited to communications, mass electronic data storage, image analysis, unmanned aerial vehicles, and license plate readers. A multi-faceted analytical framework that accounts for investigatory, policy, privacy, technology, or resource-related requirements, constraints, and other factors will enable agencies with limited resources to leverage the information and resources of the NDCAC to make systematic and informed technological decisions. Over time, this role may enable the NDCAC to coordinate the aggregation of model policies or decision-making guides relating to discrete technologies or consideration checklists designed to inform law enforcement agencies on benefits, costs, risks, or threats presented by significant emerging or morphing technologies. Additional resources should be commensurate in breadth to the expanded mission.

6.4.3 The National Domestic Communications Assistance Center should serve as a clearinghouse for information and resources regarding the lawful recovery of stored digital evidence in consumer technologies and other technologies impacting law enforcement.

The NDCAC should expand its current secure online knowledge repository of information to include a broader set of technologies and technological issues important to the law enforcement community, both which affect investigatory and operational aspects of law enforcement's mission. The online portal should include timely and technology-specific analytical frameworks for agencies to use in their decision-making regarding emerging or morphing technologies. The online repository allows the NDCAC to make information available to all registered law enforcement personnel. In addition, the NDCAC (and in the past the FBI's OTD) had previously published for law enforcement an *Emerging Technology Review Bulletin* in a format not unlike the *FBI's Law Enforcement Bulletin*. The *ETR Bulletin*, as it was known, was a compendium of plain language explanations of emerging technologies and their potential or actual impact, positive or negative, to law enforcement. The NDCAC should revive this publication and distribute it through traditional print and digital format on its online knowledge repository, and disseminate it across federal, state, and local law enforcement agencies. The *ETR Bulletin* would serve a complementary, bi-annual compendium of the most significant research done by the NDCAC.

6.4.4 The National Domestic Communications Assistance Center should provide broad, inexpensive and

easily accessible training to local, state, and federal law enforcement agencies in applicable forensic or digital analytical recovery techniques, and other technologies that have an impact on law enforcement.

The NDCAC currently offers periodic technology and digital forensic training sessions on a limited basis to state and local officers. The NDCAC's training efforts have been recognized within and outside of the law enforcement community. The Intelligence Commanders Group (ICG) of the Major Cities Chiefs Association (MCCA) and Major County Sheriffs of America (MCSA) recognized the NDCAC training efforts in a recent report. In its Report, the ICG stated the NDCAC "is a tremendously valuable resource, since it is not practical or possible for every one of the thousands state and local law enforcement agencies across the country to have, within their own department, adequate access to resources and expertise."[36] The Center for Strategic and International Studies (CSIS) developed a report[37] highlighting potential solutions to law enforcement's challenges with digital evidence, while specifically leaving the challenge of encryption out of the report's scope. CSIS conducted extensive interviews with law enforcement officials, technology company representatives, and others, and recommended, "Congress can and should adequately resource NDCAC to serve the training and technical roles that already fall within its mission." NDCAC should expand both the scope and volume of its training to include a broader range of technologies impacting law enforcement as well as exploring new vehicles and methodologies for delivering training. Current courses such as "Best Practices for Collection/Seizure of Mobile Devices for Investigations" and "Understanding Investigating Techniques for Modern Telecommunications" should be complemented by courses reflective of an expanded set of technological issues and challenges. The effect, over time, will be to elevate law enforcement's ability to lawfully access that digital evidence which is accessible despite impenetrable encryptions.[38]

6.5 Facial Recognition Technology

Background

PULL QUOTE: "Evolving technology such as facial recognition software will play a critical, and growing, role in investigating and preventing crimes. Law enforcement agencies, however, must ensure that the use of this investigative tool is tempered by the respect for constitutional, privacy, and civil rights of free citizens. Requiring that officers be trained on appropriate use, the tool's limitations, and promoting transparency, will properly balance these interests."[39] - BJay Pak, United States Attorney, Northern District of Georgia

Facial recognition technology (FRT) refers to digitally matching images of faces from one image to find a matching image.[40] The technology to compare two images using a computer algorithm has been in

[36] Major Cities Chiefs Association. 2018. Richardson, Tara. Critical Issues for Intelligence Commanders: Preventing Terrorism and Targeted Violence and Maintaining Access to Digital Evidence, page 43.
[37] Center for Strategic and International Studies (CSIS) *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge* (https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge)
[38] The prioritized access of so-called "low hanging fruit" by law enforcement may assist, but will never fully substitute for access to encrypted content when authorized by court order. The spoken or written words of a defendant or co-conspirator will always be the most compelling evidence of the objective truth of an offender's guilt or innocence.
[39] BJay Pak, United States Attorney Northern District of Georgia, email Communication with Federal Program Manager, Joe Heaps, April 30, 2020.
[40] See Andrew Gutherie Ferguson, *Facial Recognition and the Fourth Amendment* available at SSRN ID 3473423) * 6

development for close to 40 years.[41] It works by creating a digital "face print" of a subject and seeks to match the print to a known image of a person:[42]

> When one digital representation of a face is compared to another digital representation of a face and the code lines up the same, the computer will deem the process a match. These digitized images are stored in large datasets so that a computer model can train itself on what constitutes a "match." In many systems, returned "matches" involve more than one image and may involve as many as 20-50 similar face prints. These face images are provided in order of the closeness of an overlap of the fixed digital features.[43]

Military and intelligence communities were early adopters of this FRT, and law enforcement greatly expanded the use of FRT over the last decade.[44] When combined with a system of cameras, FRT can help law enforcement investigate crimes, reduces the pool of persons of interest and suspects, exonerates the innocent, and maximizes limited law enforcement resources.

While this technology has been under development for some time, it is one of the pre-eminent technologies that must be examined, refined, and appropriately implemented given the role it may play in law enforcement over the next decade. Concurrently, its use must be transparent and appropriately secure individual's civil liberties and privacy.

Current State of the Issue

Law enforcement agencies use FRT in three general ways: field use, custodial and supervisory use, and investigative use.[45] Field use includes using FRT to identify a deceased victim, a fugitive, or an individual attempting to use a fake identification to commit identity or other types of fraud.[46] Custodial and supervisory use includes using FRT as a form of biometric identification throughout the criminal justice process.[47] Investigative use includes applying FRT to surveillance footage or other photographs to identify potential suspects, associates, witnesses, or victims for investigative leads.

State and local law enforcement agencies most commonly use FRT for investigative purposes.[48]

---

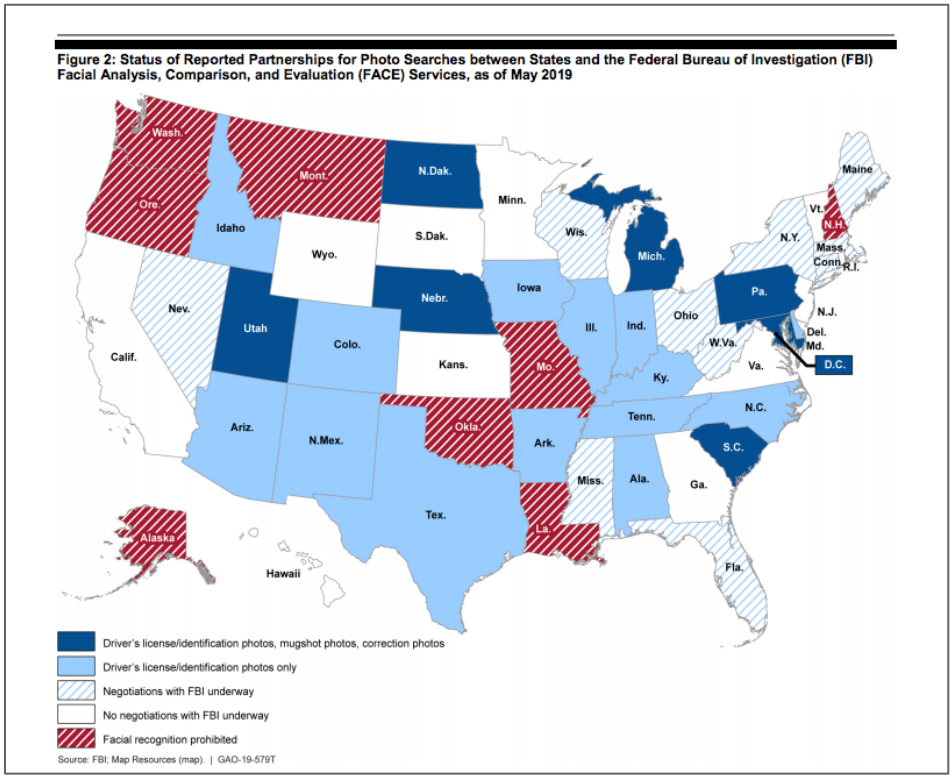
[41] Alessandro Acquisti, Ralph Gross, and Fred Stutzman, Face Recognition and Privacy in the Age of Augmented Reality, Journal of Privacy and Confidentiality 6 No. 2, at 2 (available at SSRN ID 330512)
[42] A "face print" is a digital map of one's face in computer code, much like a digitized map of the ridges and valleys of fingers in finger print technology.

[43] See Andrew Gutherie Ferguson, Facial Recognition and the Fourth Amendment (SSRN ID 3473423) at * 6.
[44] For example, Facebook claims that it has the largest facial-recognition database, and its users upload millions of photos daily. Lane Brown, There Will Be No Turning Back on Facial Recognition, New York Magazine, November 12, 2019. Available online at https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html. Facebook's facial-recognition algorithm, DeepFace, is believed to be more accurate than software used by government agencies.

[45] IJIS Institute Law Enforcement Facial Recognition Use Case Catalog, March 2019 at p.7 available at https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog

[46] *See id.* at 8-11. The Use Case Catalog contains citations to real-life examples where FRT was used out in the field to generate concrete investigative leads that resulted in a successful enforcement event. See also, A common example of Field Use is the U.S. Department of Homeland Security, Customs and Border Protection using FRT on passports or other documents presented by foreign travelers seeking to gain entry into the U.S.
[47] *See id.* at 15-16.
[48] Investigative use is similar to Face Identification usage, where law enforcement has suspicion about a particular person and an image or footage from a crime scene is matched with different photo datasets. See Andrew Gutherie Ferguson, Facial Recognition and the Fourth Amendment (SSRN) * 11.

The New York Police Department has used FRT to generate leads for persons of interest since 2011.[49] The FBI operates two FRT programs: the Next Generation Identification Interstate Photo System and the Face Analysis, Comparison, and Evaluation Service program.[50] From August 2011 to April 2019, the FBI has conducted approximately 390,000 searches on behalf of law enforcement users, with 152,565 search requests received during the period from July 2017 through April 2019. [51][52]



The growing use of FRT has not been without concern. The concerns can be grouped into three areas: privacy and civil liberties concerns, data security and hacking, and accuracy issues. Over the years, privacy advocates and academics have raised concerns about how all levels of government collects and stores photographs to support FRT, the accuracy of the matches using FRT, and how FRT and the underlying data are used and shared.[53]

---

[49] Lane Brown, There Will Be No Turning Back on Facial Recognition, New York Magazine, November 12, 2019. Available online at https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html

[50] See https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi; https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit

[51] See Statement of Gretta L. Goodwin, Director Homeland Security and Justice, U.S. Government Accountability Office, Testimony Before the Committee on Oversight and Reform, House of Representatives, June 4, 2019. Available at https://www.gao.gov/assets/700/699489.pdf

[52] https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use

[53] See Jennifer Lynch, What Facial Recognition Technology Means for Privacy and Civil Liberties, Written Testimony Submitted to the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law, at 12-15. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134497; Ashely Deeks, Facial Recognition Software: Costs and Benefits, Lawfare, March 27, 2018, available at: https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits

Entities collect a large numbers of photos of the public, often without their knowledge or consent. People also voluntarily provide photos to commercial entities (e.g., social media companies) whose terms of service allows them to be shared with third parties. When coupled with faster computing speed and access to a large database of photographs of millions of individuals, FRT can help track the movements of individuals in almost real time and can also be used to recreate their whereabouts. Such tracking may implicate an individual's First Amendment rights to free speech and association, and the Fourth Amendment rights against unreasonable searches and seizures.[54]

Additionally, some people are concerned about whether FRT data are secured against hackers or other unauthorized individuals.[55] Another concern relates to the accuracy rate of the facial recognition software, as some studies have shown that the software misidentified people of color or females at a higher rate than other groups.[56]

[BEGIN TEXT BOX]

The International Association of Chiefs of Police (IACP), in conjunction with the IJIS Institute, has adopted a set of recommendations and guiding principles related to the use of FRT.[57] These organizations recommend that the law enforcement agencies

1. fully inform the public how and when FRT is used, and how it is collected and stored
2. quickly establish use parameters to engender public confidence
3. publicize the effectiveness of FRT by citing real-life success stories
4. create best practice principles and policies[58]

The organizations also adopted some guiding principles for law enforcement agencies when contemplating the use of FRT:

Principle One: It is the responsibility of the user agency to develop appropriate facial recognition technology usage policies in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject. In response to the expanding use of new and emerging technologies, the International Association of Chiefs of Police (IACP) released a Technology

---

[54] See Lynch, at 15. Although beyond the scope of this report, it is noteworthy that recent U.S. Supreme Court's decisions in *U.S. v. Jones*, 565 U.S. 400 (2012) and *Carpenter v. U.S.* 585 U.S. ___; 138 S.Ct. 2206 (2018), seem to indicate the high Court's willingness to recognize a reasonable Fourth Amendment privacy interests may extend to data held by third parties requiring the government to obtain a search warrant to access such data.

[55] See Brown, There Will Be No Turning Back on Facial Recognition, New York Magazine, November 12, 2019. Available online at https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html

[55] See https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi;

[56] See id. at 15 ("Some have also suggested the false-positive risk inherent in large facial recognition databases could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities.")(citations omitted); Lane Brown, There Will Be No Turning Back on Facial Recognition, New York Magazine, November 12, 2019 (citing a study conducted by researchers at Massachusetts Institute of Technology that showed that some FR software from IBM, Microsoft, and Facebook were less accurate when identifying females). Available online at https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html

[57] See Law Enforcement Imaging Technology Task Force, Law Enforcement Facial Recognition Use Case Catalog, March 2019 (a joint effort of the IJIS with the IACP), available at: https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog ("Facial Recognition Use Catalog"); see also, Law Enforcement Imaging Technology Task Force, Guiding Principles for Law Enforcement's Use of Facial Recognition Technology, July 2019 (a joint effort of the IJIS with the IACP), available at https://www.theiacp.org/resources/document/guiding-principles-for-law-enforcements-use-of-facial-recognition-technology ("Guidelines")

[58] See Facial Recognition Use Case Catalog, March 2019 at 17-19.

Policy Framework to guide the development and support policies that ensure responsible and effective deployment and use of technologies.

Principle Two: All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit any use of the technology that would violate an individual's rights under the First and Fourth Amendments.

Principle Three: The results returned in a facial recognition candidate list are ranked based on computational analysis of the similarity of features. The candidate list may include photos of individuals who may be of a different race, gender, or age than the individual in the submitted probe photo.

Principle Four: The images and information contained in the candidate list are for investigative lead generation purposes only, and are not to be considered as positive identification, or used alone as the basis for any law enforcement action.

Principle Five: Before access to any facial recognition system is authorized, a law enforcement agency should require individual users to participate in training on how the facial recognition system functions, its limitations, the importance of using high resolution equipment and images, and the interpretation of results, as well as the implementation of and adherence to the agency's facial recognition policy.59

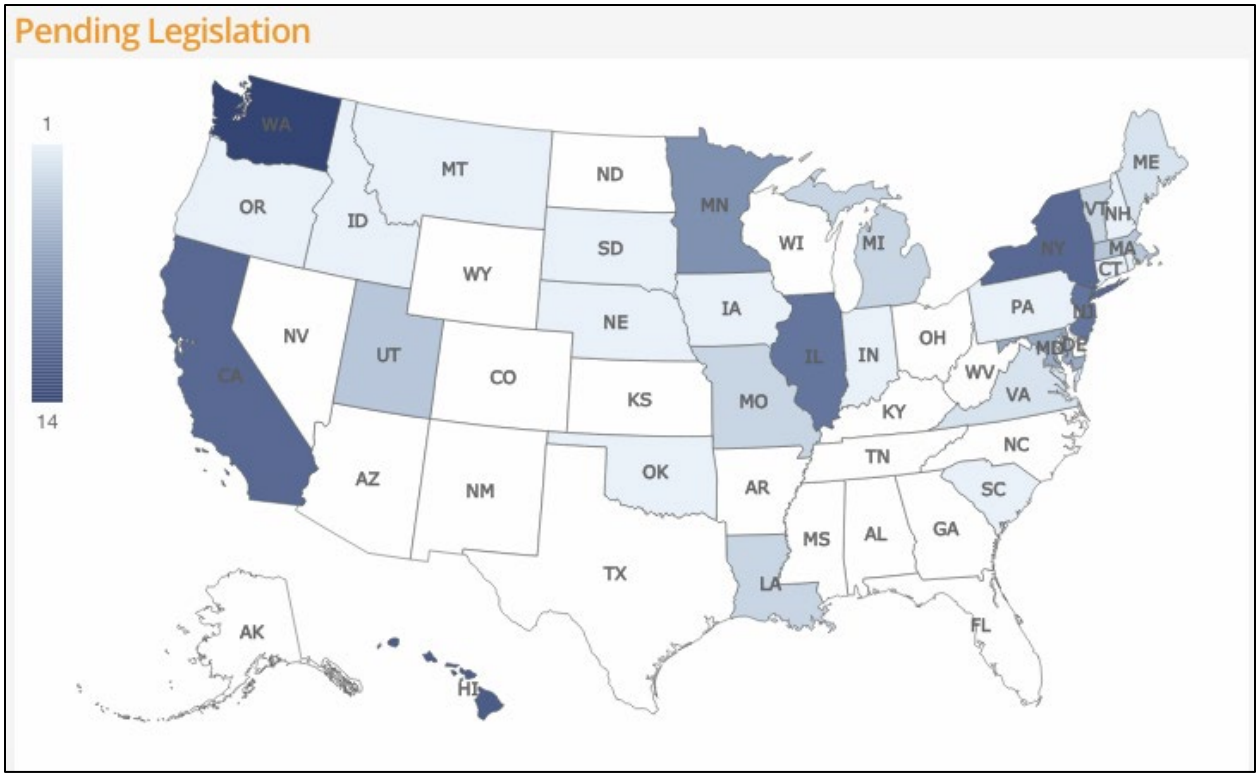
[END TEXT BOX]

[BEGIN TEXT BOX]

Some jurisdictions have rushed to pass laws or ordinances that significantly limit the use of FRT by law enforcement. In May 2019, San Francisco, California, banned the use of FRT by all city agencies.[60] Oregon,[61] New Hampshire,[62] California, [63] and Washington[64] have statutes that limit the use of FRT.

[END TEXT BOX]

[59] Guidelines at 1.
[60] https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html
[61] See O.R.S. 133.741(1)(B)(D) (Prohibiting the use of FRT to analyze recordings obtained through body worn cameras).
[62] See N.H. Rev. Stat. § 263:40-b (prohibiting the state department of motor vehicles from using FRT); § 260:14 (prohibiting the department of motor vehicles from sharing drivers license photographs with the federal government); and N.H. Rev. Stat. 105-D:2 XII (prohibiting use of FRT on body worn camera footage).
[63]See AB 1215; State of California's bans for three years the use of FRT on images captured on body-worn cameras, but permit use of FRT in other surveillance footage. See https://www.usatoday.com/story/tech/2019/12/17/face-recognition-ban-some-cities-states-and-lawmakers-push-one/2680483001/
[64] SB6280 (effective on July 1, 2021); Washington's statute requires, among other things, human review of "matches," training for personnel using FRT, and requiring a warrant to conduct real-time surveillance.



(Source: Electronic Privacy Information Center, available at www.epic.org, accessed on April 14, 2020)

Federal law does not govern the use of FRT, but several bills have been introduced in Congress.[65] Federal agencies, such as the FBI, have already adopted a set of policies to prevent the FRT abuse.[66] Key points of the FBI's policy follow:

- FBI policy strictly governs the circumstances in which facial recognition tools may be used, including what probe images may be used.
- FBI uses facial recognition technology for law enforcement purposes with human review and additional investigation. The FBI's use of facial recognition produces a potential investigative lead and requires investigative follow-up to corroborate the lead before any action is taken.
- Every face query—including results received from our partners—is reviewed and evaluated by trained examiners at the FBI to ensure the results are consistent with FBI standards.
- The FBI is committed to ensuring that FBI facial recognition capabilities are regularly tested, evaluated, and improved. In addition to system testing, the FBI has partnered with NIST to ensure algorithm performance is evaluated.[67]

[65] Jon Schuppe, New federal bill would restrict police use of facial recognition, NBC News, November 14, 2019, available at https://www.nbcnews.com/news/us-news/new-federal-bill-would-restrict-police-use-facial-recognition-n1082406

[66] See Statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, before the House Oversight and Reform Committee, June 4, 2019, available at https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use

[67] See id.

As Congress and additional state and local governments move to regulate the use of FRT, law enforcement must engage in the process early on and build a self-regulated framework prior to legislative action.

6.5.1 Federal and state governments should fund the use of facial recognition technology to assist in the prevention and investigation of criminal activities.

FRT is an efficient and effective investigative tool used to prevent and detect criminal activity. As New York Police Commissioner James O'Neill notes, "Facial recognition technology can provide a uniquely powerful tool in our most challenging investigations such as when a stranger suddenly commits a violent act on the street."[68] Law enforcement should report on successful uses of FRT.

6.5.2 Law enforcement agencies should review or adopt policies on the use of facial recognition technology.

IACP's *Guiding Principles for Law Enforcement's Use of Facial Recognition Technology* provides a good framework that agencies can use to evaluate existing practices or adopt new procedures. Agencies should focus on how to comply with constitutional principles, applicable statutes, and local laws.

6.5.3 Law enforcement agencies should educate the public on the value of facial recognition technologies and the safeguards adopted on use of such technology.

Law enforcement agencies should collect and share concrete examples of instances where the use of FRT successfully aided in the investigation or prevention of criminal activity and inform the public on steps taken to deter misuse, the amount of training required for its use, and transparency measures

Methodology

Field Visits

- List all field visits – including date, location (understood these will likely be virtual) and a very brief description of the program/agency that was observed. We'll provide general language up front on the purpose of field visits, etc…
    - Virtual SME event mid-May cancelled.

Hearings

- This can be done centrally, no action needed from FPM/WG per chapter.

Literature search

- List all databases used to search for and access relevant literature, including websites (e.g. COPS resource library), digital archives (e.g. homeland security digital library), and use of NCJRS. Also, include any outreach made to SMEs, associations, and other contacts inquiring about publications and documents pertinent to your WG.
- IACP Digital Evidence Task Force Executive Primer
- Fiscal Year 2020 SAFECOM Guidance on Emergency Communications Grants
- IACP NATIONAL LAW ENFORCEMENT POLICY CENTER Body-Worn Cameras Concepts and Issues Paper

[68] https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html

- Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks. Washington, DC: Office of Community Oriented Policing Services.
- Task Force on Optimal (Public Safety Answering Point (PSAP) Architecture (TFOPA) A Federal Communications Commission (FCC), Federal Advisory Committee, Adopted Final Report, Washington, DC, 2016.
- National 911 Progress Report
- 911 Data & Information Sharing: A Strategic Plan

SME briefings

Facial Recognition Subject Matter Experts 1 PM April 22, 2020

Presenters

- Jennifer Lynch Surveillance Litigation Director at the Electronic Frontier Foundation
- Jake Laperruque Senior Counsel at The Constitution Project at Project On Government Oversight (POGO)

Facial Recognition Subject Matter Experts 3 PM April 22, 2020

Presenters

- Brian Hennessey Head of our Special Investigations Unit, NYPD
- Oleg Chernyavsky, Assistant Deputy Commissioner Legal Matters, NYPD
- Michael Clarke, Managing Attorney Legislative Affairs Unit, NYPD

Unmanned Aircraft Systems Subject Matter Experts 3 PM April 22, 2020

Presenters

- Adam B. Ringle, M/Sgt., Wilmington Police Department
- Roxana Kennedy, Chief, Chula Vista Police Department
- Vern Sallee, Captain, Patrol Operations Division, Chula Vista Police Department

Lawful Access Subject Matter Experts 1:30 PM May 15, 2020

Presenters

- Elizabeth Banker, Deputy General Counsel, Internet Association
- Stewart Baker, Host, Steptoe & Johnson LLP's *Cyberlaw Podcast*

Moderator

- Executive Assistant Director Darrin E. Jones, Science and Technology Branch, Federal Bureau of Investigation

Data

- List any datasets which were reviewed, referenced in your WG deliberation – including title of the dataset, year, and description of how/what part of your WG activity it informed, and include a hyperlink to the dataset. Assuming here that there hasn't been any data analysis for any of the chapters. If there is, please discuss with your team lead.

Business meetings (conference calls)

- Business meetings should include any standing or ad hoc call for your entire WG, or a defined subset, to discuss commission work and/or hear SME testimony
- Include complete list of meetings held, including dates

- Work Group Meeting 1 21 February 2020
- Work Group Meeting 2 28 February 2020
- Work Group Meeting 3 6 March 2020
- Work Group Meeting 4 13 March 2020
- Work Group Meeting 5 20 March 2020
- Work Group Meeting 6 27 March 2020
- Work Group Meeting 7 Scheduled 3 April 2020
- Work Group Meeting 8 Scheduled 10 April 2020
- Work Group Meeting 9 Scheduled 17 April 2020
- Work Group Meeting 10 Scheduled 24 April 2020
- Work Group Meeting 11 Scheduled 1 May 2020
- Work Group Meeting 12 Scheduled 8 May 2020
- Work Group Meeting 13 Scheduled 11 May 2020
- Met with Reduction in Crime Work Group 1 April 2020
- Met with Data and Reporting Group Scheduled 7 April 2020

References

U_FOUO
TechnoloAdoption Fra