## Chapter 6. Technology

### Introduction

Advances in technologies have created opportunities and efficiencies in many aspects of our daily life. Such advances have spawned new forms of connectivity and commerce, bringing people around the world together in ways not imagined or technologically possible just a decade ago. However, these technologies have opened a new world for exploitation by criminals, terrorists, and spies.

Attorney General William P. Barr addressed these issues at the Lawful Access Summit in Washington, DC, in October 2019:

> "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."[1]

To stay ahead of criminals and threats to the American public, law enforcement is working to leverage technology in response to the criminal exploitation of technology and to enhance their crime reduction efforts more generally. Emerging technologies present a great opportunity to increase law enforcement capacity to carry out their mission to uphold the rule of law. However, prior to adopting new technologies, law enforcement agencies should examine, the potential risks and costs associated with implementing a particular technology. Furthermore, since 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 require strong cybersecurity risk frameworks. Agencies must diligently employ and routinely audit their mitigation strategies to ensure effective implementation and actual risk reduction.

To assess the potential implementation of a new technology, the Commission recommends that law enforcement agencies develop and use a framework. A framework offers a starting point for law enforcement executives to identify the most critical concerns and the specific considerations related to the technology or advancement. The term "framework" represents a carefully considered, methodical, and repeatable approach law enforcement agencies may use to consider the adoption of a new technology. This tool guides law enforcement executives through certain decision-making processes, to assess the pros, cons, and other predictable considerations of the technology.

This chapter highlights several potential new technologies for law enforcement agencies to consider for implementation and includes recommendations on how agencies should assess adopting these technologies. However, this chapter does not discuss in detail all of the current technological tools available to law enforcement. Certain other technologies like the National Integrated Ballistics Information Network (NIBIN), Crime Gun Intelligence Centers (CGICs), and automatic license plate readers (ALPRs) are discussed in the Reduction of Crime chapter of this report instead.

**[CROSS REFERECENCE TO REDUCTION OF CRIME]**

### 6.1 Lawful Access

**PULL QUOTE:** "The impact and magnitude of the lawful access crisis in the United States has grown to a point

[1] William P. Barr, U.S. Attorney General, "Remarks as Prepared for Delivery," presented at the Lawful Access Summit, Washington DC, October 4, 2019, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit.

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."[2] - Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation

A growing number of U.S. tech companies have already or promise to transition from managed strong encryption models to user-access only and end-to-end encryption models, which by design prevent court-authorized lawful access to evidence.[3] If the end user is a criminal or terrorist, these products and services may help them hide or protect 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 valid warrant or court order. This creates a lawless space that criminals, terrorists, spies, and other bad actors can exploit,

As more and more companies transition to these user-access only and end-to-end encryption models, the lawful access of otherwise accessible, court-authorized information becomes restricted. While most publicized instances of this relate to the FBI and terrorism, it must not be overlooked that state and local law enforcement also encounters these types of encryption challenges daily. The impact of user-access only and end-to-end encrypted data increases the number of unsolvable crimes and denies justice for victims. In addition, it threatens to dramatically affect the nation's dual-sovereign federal system of law enforcement. When police and sheriffs cannot gain lawful access to critical criminal evidence that has been encrypted, they will have to turn for assistance to larger federal agencies whose own resources are already taxed.

In March 2019, Facebook announced its intention to encrypt Facebook Messenger.[4] Facebook provides more reports to the National Center for Missing and Exploited Children (NCMEC) than any other tech company, with more than 15 million CyberTipline reports a year.[5] While the commission recognizes and applauds Facebook's substantial efforts to combat these crimes against children, it is discouraged 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 electronic service providers (ESP);

[2] *President's Commission on Law Enforcement and the Administration of Justice: Hearing on Reduction of Crime* (April 15, 2020) (written statement of Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

[3] Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, June 10, 2020. On April 1, 2020, Zoom, a major online video-conferencing provider made popular by the COVID-19 pandemic, issued a public statement describing how they use server-to-server encryption to maintain security for customers but also stated, "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"; Oded Gal, "The Facts Around Zoom and Encryption for Meetings/Webinars," *Zoom* (blog), April 1, 2020, https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/. On May 7, 2020, Zoom announced their intent to deploy end-to-end encryption. At that time, Zoom added, "Zoom has not and will not build a mechanism to decrypt live meetings for lawful intercept purposes"; Eric S. Yuan, "Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering," *Zoom* (blog), May 7, 2020, 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/.

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

[5] Priti Patel, William P. Barr, Kevin K. McAleenan, and Peter Dutton to Mark Zuckerberg, Chief Executive Officer, Facebook, October 4, 2019, U.S. Department of Justice, https://www.justice.gov/opa/press-release/file/1207081/download.

[6] *President's Commission on Law Enforcement and the Administration of Justice: Hearing on Juvenile Justice* (May 4, 2020) (written statement of John Clark, President and Chief Executive Officer, National Center for Missing and Exploited Children), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

members of the public; federal, state, and local law enforcement; and prosecutors combat online child sexual exploitation."[7] – John Clark, President and CEO, The National Center for Missing and Exploited Children

**[END TEXT BOX]**

Historically, law enforcement has typically relied upon the tech industry to help identify and transfer specific information to officials, as directed by a court-ordered search warrant. This 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. In addition, the practice levels the enforcement playing field by giving access to state and local law enforcement agencies that are less likely than federal agencies to have the technological expertise to execute the order without such assistance.

For many years, Apple and Google routinely granted law enforcement lawful access to their operating systems when they received a court-ordered search warrant. That changed in 2015 when Apple rolled out an operating system designed to make the content of its smart phones inaccessible by anyone except the user. Soon, other providers followed suit. Companies that have chosen to adopt end-to-end user encryption have effectively upended more than 200 years of jurisprudence by placing evidence beyond the reach of a court-ordered search warrant. The criminal justice system has been weakened and law enforcement's ability to protect and promote the public's safety has been handicapped. In order to ensure that law enforcement can access all the relevant information it needs in the course of their work investigating crimes the issue of lawful access must be resolved. The following recommendations offer solutions towards this end.

### 6.1.1 Congress should require providers of communications services and electronic data storage manufacturers to implement strong, managed encryption for stored data and data in motion, while ensuring lawful access to evidence pursuant to court orders.

The Communications Assistance for Law Enforcement Act (CALEA) has not kept pace with the realities of today's modern internet and the public's near abandonment of the traditional telephone network.[8] In today's reality of always available ways to communicate, app providers have not merely replaced a portion of the local telephone exchange; they have effectively become the local telephone exchange. Yet, several app providers bear no social or legal responsibility to compensate for or curb the harms caused by criminal elements that they know routinely use their services and products with an impunity facilitated by their designs.

Despite years of candid discussions initiated by law enforcement with a number of these providers and manufacturers, the companies have made little progress to resolve lawful access issues voluntarily. Instead, during that period, the problem has worsened and threatens to become the norm. It has become evident that a legislative solution is therefore necessary.

Additionally and just as significantly, 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 by paying more of the costs associated with their inaction. While tools like artificial intelligence (AI) offer some promise to help detect and prevent some online crime, a lack of actionable evidence may still leave law enforcement unable to act, which leaves victims unable to achieve justice.

[7] Clark, *President's Commission on Law,* May 4, 2020.[8] "Communications Assistance for Law Enforcement Act," Federal Communications Commission, last modified March 24, 2020, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance; Communications Assistance for Law Enforcement Act, 47 U.S.C. §1001 (2006), https://www.law.cornell.edu/uscode/text/47/1001.

[8] "Communications Assistance for Law Enforcement Act," Federal Communications Commission, last modified March 24, 2020, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance; Communications Assistance for Law Enforcement Act, 47 U.S.C. §1001 (2006), https://www.law.cornell.edu/uscode/text/47/1001.

The commission considered but rejected the idea that lawful access equates to back-door access. Almost all mobile device manufacturers, operating system vendors, and app providers maintain their own "upgrade" back doors, which enables providers to routinely change functions and settings of a device or service. Law enforcement does not seek such direct access, nor does it wish to hold any encryption "keys." Instead, law enforcement seeks to have tech companies develop and manage for themselves the capability to respond to a lawful court order. Having tech companies themselves remain in control of this process is actually privacy enhancing, ensuring law enforcement is afforded only specific, limited access to data as defined in each case by a specific warrant.

Major financial institutions both in this country and abroad engage in billions of dollars of transactions daily, and the security of these transactions is maintained and managed through strong encryption, yet these institutions also maintain the ability to access such information when lawfully justified. This duality suggests that the issue is not one of technological impossibility, but a question of willingness on the part of the tech industry. The commission concurs with the December 2019 resolution of the IACP, which calls for worldwide legislation that compels companies to develop for themselves and implement appropriate lawful access capabilities for their products and services.[9]

Civil liability immunity statutes that were adopted during the infancy of many tech companies may unintentionally encourage such companies to pursue and market user-access only and end-to-end encryption models. Absent any risk of financial liability, the routine cost−benefit analysis—which most companies use to determine whether to dedicate resources to harm-mitigation strategies—may not influence some of these technology companies into a willingness to facilitate lawful access.

As long as tech companies are immune from liability, the commission assumes that these companies perceive any development or maintenance of lawful access capabilities to be a drain on profits, which allows the tech companies to hide their financial motivations under the guise of a desire to enhance users' privacy. Ultimately, this behavior enables plausible corporate ignorance and allows criminals to use these systems for illegal purposes. If corporations are to continue to benefit from civil immunity, Congress should mandate that these companies develop and maintain a lawful access solution capable of producing clear text data in response to court-ordered search warrants.

### 6.1.2 Congress should implement regulations and laws that require internet service providers and companies that provide commercial virtual private network services to retain certain records and set record retention periods.

The Stored Communications Act (SCA) of 1986 requires data to be stored for up to 180 days upon request by the government. Providers must also disclose private information in emergency cases where individuals or groups may be in danger. In addition, a "court order is required for access to digital information. An administrative subpoena may be issued to gain access to specific data such as usernames, addresses, telephone numbers, and call transcripts."[10]

Recently, the FBI investigated a gang task force case where it was revealed that the primary suspect of a homicide case used FaceTime to orchestrate the crime. Because Apple uses end-to-end encryption, it allows criminals to coordinate their crimes through this avenue. If law enforcement is given lawful access, they can then intercept the plans of criminals and gain evidence to prosecute those who break the law.

### 6.1.3 The FBI should establish a Lawful Access Technology Resource Center. The FBI should restructure the National Domestic Communications Assistance Center's Executive Advisory Board to allow law

[9] International Association of Chiefs of Police, *IACP 2019 Resolutions Adopted* (Alexandria, VA: International Association of Chiefs of Police, 2019), https://www.theiacp.org/sites/default/files/Adopted%202019%20Resolutions Final.pdf. The paragraph refers to Resolution 21 of the Internal Association of Chiefs of Police December 2019 Resolutions. [10] "How Data Retention Legislation Impacts VPN Providers for the Better," Finjan Mobile (blog), August 1, 2017, https://www.finjanmobile.com/how-data-retention-legislation-impacts-vpn-providers-for-the-better/.

[10] "How Data Retention Legislation Impacts VPN Providers for the Better," Finjan Mobile (blog), August 1, 2017, https://www.finjanmobile.com/how-data-retention-legislation-impacts-vpn-providers-for-the-better/.

**enforcement executives from federal, state, local, and tribal law enforcement agencies to address specific and sensitive law enforcement matters, including the impact and development of emerging technologies on law enforcement operations.**

The pace of both the evolution and iteration of technologies can potentially both assist and challenge law enforcement. However, few local law enforcement agencies have the resources to keep abreast of this evolution on an ongoing basis. These agencies need an enduring, shared, collaborative structure that can serve as a hub for technical knowledge management and the exchange of solutions and knowledge among law enforcement agencies.

Established by the FBI, the National Domestic Communications Assistance Center (NDCAC) opened in 2013 to help federal, state, local, and tribal law enforcement keep abreast of the communications revolution.[11] The NDCAC is a core FBI-sponsored technology group composed of engineering personnel, contractors, and technically trained law enforcement officers. The NDCAC also has access to and collaborates with engineers and technical staff of the FBI's Operational Technology Division (OTD), which conducts court-ordered wiretaps and the forensic search of stored electronic information. However, as currently structured, the NDCAC focuses almost exclusively on issues involving real-time lawful interception and the recovery of stored communications. If restructured it could be leveraged to help law enforcement agencies collaborate to address challenges with lawful access.

The NDCAC's current mission and resources are inadequate to fully confront, track, assess, and generate recommendations to address the rapidly evolving challenges of modern technologies on a larger scale. By restructuring the NDCAC, law enforcement executives from federal, state, local, and tribal law enforcement agencies would be able to utilize it to help them address a broader range of sensitive law enforcement technology matters, like lawful access.

Additionally, 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 that have an impact on law enforcement.

The NDCAC should expand its secure online knowledge repository to include a broader set of technologies and technological issues that are important to the law enforcement community. The online portal should include timely and specific analytical frameworks for agencies to use for emerging or morphing technologies. All registered law enforcement personnel should be able to access the online repository, and the NDCAC should include all important information on its portal. This restructuring would also allow the National Domestic Communications Assistance Center to provide broad, inexpensive, and easily accessible training to federal, state, local, and tribal law enforcement agencies in applicable forensic or digital analytical recovery techniques and other technologies that have an impact on law enforcement.

Training is one of the most crucial ways to address the challenges of today's technologies. Law enforcement officers and prosecutors must be trained to understand the impact of and to properly leverage new and evolving technologies.

The NDCAC should expand both the scope and volume of its training to include a broader range of technologies that have an impact on law enforcement.

### 6.3 Implementing New Technologies

From the adoption of multi-shot pistols in the 1830s to the creation of soft body armor in 1972 to the emergence of crime mapping computer programs in the 1990s, technology has always been interwoven into how policing is conducted. However, today there is a vast array of possible innovative technologies and advancements that law enforcement could leverage in their work. Sifting through which of these could actually be useful to their agency can be burdensome, and even once a technology is decided on the

[11] "About," National Domestic Communications Assistance Center, accessed June 30, 2020, https://ndcac.fbi.gov/about.

acquisition and implementation of it adds further layers of complexity—not to mention significant costs in the face of budgetary constraints. Deployment of new technologies can also raise other issues for consideration, including public acceptance and constitutional and legal concerns. But despite these challenges, technology can bring enormous benefits to law enforcement agencies, to make their work more efficient or less dangerous, to better capture and analyze evidence, to get faster leads for investigations, to intercept crimes, to identify and catch criminals, and many more. These recommendations offer some possible technologies for law enforcement to consider implementing that have been shown to be successful in enhancing law enforcement's work of combatting crime.

### 6.3.2 Law enforcement should consider the use of Unmanned Aircraft Systems (UAS) as a tool for fighting crime.

Law enforcement and public safety agencies across the country recognize that drones can be a tool in fighting crime and that their use can protect and save officers' lives. For example, one evening in August 2017, an officer from the Wilmington (Delaware) Police Department was working with an agent from Delaware Probation and Parole when gunshots were fired in their direction. Subsequently, the incident drew a significant law enforcement response, including officers and tactical teams from surrounding jurisdictions.[12]

The search for the gunman led officers to an alley where they heard sounds; it was fenced in and largely obscured from view. Given the lack of visibility, a tactical team breaching the alleyway would have put officers at risk if the suspect had been present. The team deployed a drone equipped with an on-board thermal imaging camera, which was able to show that the movement came from a dog in the alley, rather than an armed gunman. The use of a drone in that situation kept officers from further harm and possibly being surprised by the dog and potentially discharging a weapon. Simultaneously, the drone provided the situational awareness needed, without a single person being at risk.[13]

Law enforcement agencies though should thoroughly research and consider the full range of policy, legal, constitutional, and ethical implications when adopting UAS technology. Agencies should also consider the impact of privacy and civil liberties and should engage with members of the community and other law enforcement agencies, as appropriate, that are associated with adopting this new technology.

In addition to assessing how the use of the new technology may affect external parties, law enforcement agencies should also consider the impact on its own personnel and agency resources. It is possible the technology will have other benefits, such as helping officers interact with the public, assisting the agency in using its resources better, improving response times, or helping to de-escalate events. As evidenced by the Chula Vista Police Department's (CVPD) experience with UAS in California, introducing the technology directly supported the officers' ability to de-escalate otherwise difficult response efforts.[14] The CVPD also uses drones to respond to 911 calls, with the UAS response time being less than three minutes.[15]

### 6.3.5 Law enforcement agencies should consider implementing gunshot detection technologies to combat firearm crime and violence.

An example of an emerging technology which may have unanticipated benefits is acoustic detection

[12] Robert Tracy, Chief, Wilmington Police Department, DE, email communication with Josephine Debrah, Report Writer, and Joe Heaps, Federal Program Manager, Technology Working Group, April 1, 2020.

[13] Tracy, email communication with Josephine Debrah, April 1, 2020.

[14] Verne Sallee, "Drone as a First Responder: The New Paradigm in Public Safety," *Police Chief Magazine*, March 2020, https://www.policechiefmagazine.org/drone-as-a-first-responder/.

[15] "HigherGround," HigherGround, accessed June 1, 2020, https://www.higherground.com/; "UAS Drone Program," Chula Vista Police Department, accessed June 1, 2020, https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program; and Vern Sallee, Patrol Operations Division Captain, Chula Vista Police Department, CA, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, June 9, 2020. [16] Jillian Carr and Jennifer L. Doleac, "The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data," Brookings, April 27, 2016, https://www.brookings.edu/research/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/.

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 investigative and evidentiary gains that can result from the implementation of this technology, another outcome is that police learn of nearly every firearm discharge. A 2016 Brookings Institute study reported that more than 80 percent of gunfire in the two cities studied went unreported to police.[16] As a result, police lack a full awareness of shots-fired incidents, which may include failed shootings that may be attempted again, and the community may assume that 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. The 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. Acoustic detection technology uses sensors to detect gunfire and allows analysts to pinpoint the location and immediately provide that information to police. This technology has allowed officers to decrease their response time to complaints and incidents.[17]

### 6.3.X The Department of Justice should provide funding to expand real time crime centers (RTCCs) throughout the nation and develop technology tools that provide RTCCs with the ability to identify and disseminate crime intelligence, analyze crime patterns, and develop strategies for reducing crime.

Too often, local law enforcement agencies operate as silos, rarely sharing critical data from agency to agency. However, regional real-time crime centers (RTCCs) offer a cost-efficient option, better equipping local police to fight violent crime. A RTCC is a centralized location where dedicated personnel are housed and equipped with a range of technology tools, access to data, and analytic capabilities.[18] In the past 15 years, RTCCs have grown in number and evolved in sophistication to provide a broad range of assistance to law enforcement agencies, such as surveilling public spaces via video-feed, identifying suspicious behavior in real time, and disrupting criminal networks. Commonly, RTCC technology includes video screens that display feeds from cameras throughout the jurisdiction, gunfire detection systems, and automated license plate readers (ALPR). Continual monitoring are core features of virtually all RTCCs, leading to improved decision-making and more effective operations.[19]

In recent years, RTCCs have expanded to smaller cities.  In Alabama, the average size of the law enforcement agency is 10 officers or fewer, and these smaller departments do not have access to cutting-edge technology to fight crime. Chief Bill Partridge of the Oxford (Ala.) Police Department explained how the East Metro Area Crime Center (EMACC) uses and shares advanced technology with its 28 regional partners throughout north-central Alabama, including pole cameras, camera trailers, ALPR, crime-tracing software, phone and computer forensics, and facial recognition software. Launched in May 2019, the center uses a large video wall to monitor cameras, while on-site gunshot detection and shell casing analysis can also reduce crimes. Child

[16] Jillian Carr and Jennifer L. Doleac, "The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data," Brookings, April 27, 2016, https://www.brookings.edu/research/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/.

[17] Robert Tracy, Chief of Police, Wilmington Police Department, DE, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, May 15, 2020.[18] "The Mission and Function of a Real Time Crime Center," Office for Justice Programs. https://it.ojp.gov/CAT/Documents/MissionofaRTCC.pdf.

[18] "The Mission and Function of a Real Time Crime Center," Office for Justice Programs. https://it.ojp.gov/CAT/Documents/MissionofaRTCC.pdf.

[19] John S. Hollywood et al., *Real-Time Crime Centers in Chicago: Evaluation of the Chicago Police Department's Strategic Decision Support Centers* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3242.html.

abuse is also investigated through the center's cybercrimes unit.[20]

Chief Bill Partridge of Oxford, Alabama, spoke to the commission about the East Metro Area Crime Center (EMACC), a regional RTCC launched in May 2019. He noted that EMACC provides data access and analytic services for 28 federal, state, and local public safety agencies in the northeast portion of Alabama, relying on state-of-the-art technology to provide real-time intelligence.[21]

**PULL QUOTE:** "[By bringing] these smaller departments together . . . we've seen dramatic decreases in crime, especially violent crime, across the region."[22] - Chief Bill Partridge, Oxford Police Department, Alabama

**[CROSS REFERENCE CRIME REDUCTION]**

While much of the attention paid to RTCCs focuses on data and advanced analytical tools, trained crime and intelligence analysts add important human intelligence. They use their skills to leverage core technologies, including geographic information system technology for mapping crime and assessing hotspots, software to perform link analysis or social network analysis, and statistical algorithms for assessing offender dangerousness and likelihood to offend based on past criminal history.

As technology has advanced, RTCCs have become more proficient in using unstructured data for intelligence and analysis purposes, including advanced digital media tools. Some RTCCs use sophisticated artificial intelligence solutions that automatically detect patterns of suspicious activity on video feeds, freeing the analyst from having to watch a wall full of video screens.

As documented by the Rand Corporation, adding RTCCs helps law enforcement agencies improve decision making and awareness of their communities and helps them carry out more effective, efficient operations that lead to crime reduction.[23] DOJ funding may accelerate the spread of RTCCs and increase the ability of local and state law enforcement agencies to leverage analytic and data-sharing benefits. It may also help ensure that current RTCCs are sustainable and able to adapt as technologies and data analysis approaches evolve.

To support RTCCs, DOJ could develop tools such as hardware, analytics software, and intelligence platforms. Since the Justice System Improvement Act of 1979 was enacted, the DOJ has developed standards for such technologies and helped ensure that law enforcement agencies have access to them. In addition, the DOJ administers grant programs to help bring new equipment to market by funding research and development of innovative technologies.

### 6.3.X Law enforcement agencies should thoroughly consider the full range of potential legal, constitutional, and civil liberties and privacy implications associated with generating, acquiring, or using a new technology or data set.

Within the last few years, the volume of third-party data available for resale to public and private entities has grown exponentially.[24] 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, legal restrictions may apply when the data are obtained or used by law enforcement for investigative purposes. In addition to considering commercial

[20] *President's Commission on Law Enforcement and the Administration of Justice: Hearing on Reduction of Crime* (April 16, 2020) (written statement of Bill Partridge, Chief of Police, Oxford Police Department, AL), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

[21] Partridge, *President's Commission on Law*, April 16, 2020.[22] Partridge, *President's Commission on Law*, April 16, 2020.

[22] Partridge, *President's Commission on Law*, April 16, 2020.

[23] John S. Hollywood et al., *Real-Time Crime Centers in Chicago: Evaluation of the Chicago Police Department's Strategic Decision Support Centers* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3242.html.

[24] Max Freedman, "How Businesses Are Collecting Data."[25] *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

restrictions on use, privacy and civil liberties concerns are frequently implicated by how data are stored and managed. As such, law enforcement agencies will need to consider data use safeguards, auditing, and strong data protection regimes.[25]

### 6.5 Facial Recognition Technology

**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."[26] - BJay Pak, United States Attorney for the Northern District of Georgia

Facial recognition technology (FRT) refers to digitally matching images of faces to find a matching image.[27] The technology to compare two images using a computer algorithm has been in development for nearly 40 years.[28] It works by creating a digital "faceprint" of a subject and seeks to match the print to a known image of a person:[29]

#### 6.5.1 Federal and state governments should further investigate the use of facial recognition technology to help prevent and investigate criminal activities.

FRT is an efficient and effective investigative tool used to prevent and detect criminal activity. As former 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."[30]

This technology has expedited how persons of interest are identified by helping to identify those present at the incident, while also excluding and exonerating others by confirming the alibis of those who were not there. The ability to efficiently generate investigative leads allows law enforcement to leverage their limited resources. In addition, the use of FRT can confirm any eyewitness identification of the perpetrator, which increases the credibility of such testimony and raises the confidence level of any resulting conviction.

At the same time to minimize any potential misuse and to allay these concerns, law enforcement agencies that currently use or are contemplating the use of FRT on a more regular basis should adopt governing policies on FRT.

[25] *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

[26] BJay Pak, U.S. Attorney, Northern District of Georgia, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 30, 2020.[27] Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," Abstract, *Minnesota Law Review* 105 (updated 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423.

[27] Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," Abstract, *Minnesota Law Review* 105 (updated 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423.

[28] 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 (2014), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiGrossStutzman-JPC-2014.pdf.

[29] Kevin Bonsor and Ryan Johnson, "How Facial Recognition Systems Work," How Stuff Works, accessed August 13, 2020, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm. [30] James O'Neill, "How Facial Recognition Makes You Safer," *New York Times*, June 9, 2019, https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.

[30] James O'Neill, "How Facial Recognition Makes You Safer," *New York Times*, June 9, 2019, https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.