Chapter 6. Technology

## Introduction of the Issue

**PULL QUOTE:** "The advances in various technologies are having the most dramatic impact on the way we do business since I began nearly 50 years ago! The moral, ethical, and legal ramifications of law enforcement use of various technologies must be weighed. The decisions to purchase or use technologies, therefore, must be made after careful and reasoned consideration.[1]" – Sheriff Al Cannon, Charleston County, South Carolina, Sheriff's Office

Advances in consumer product technologies have created opportunities and efficiencies in many aspects of 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.[2]

To stay ahead of criminals and threats to the American public, law enforcement must identify the benefits, risks, and costs from technology and use technology strategically and in a manner that protects the safety and civil liberties of their communities. 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, the risks and costs associated with the adoption of new technologies must be addressed prior to law enforcement's use.

**PULL QUOTE:** "Technology is an ever-increasing part of the tools utilized by law enforcement and other public safety entities. As technology evolves, a proper balance of the needs of the protectors and the rights of citizens needs to be continually assessed. Technology that is properly used can help to reduce crime rates, victimization, as well as clear innocent individuals as a suspect of wrongdoing." - John Ortolano, Chief of Police, Hobbs, New Mexico[3]

---

[1] Al Cannon, Sheriff, Charleston County, SC, Sheriff's Office, email message to Technology Working Group Report Writer, Josephine Debrah, April 10, 2020; Al Cannon, Sheriff, Charleston County, SC, Sheriff's Office, email communication with Joe Heaps, Federal Program Manager, Technology Working Group Federal, June 18, 2020.

[2] 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.

[3] John Ortolano, Chief of Police, Hobbs, NM, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 27, 2020.

The commission received information about an array of topics within the technology field, such as advanced ballistic-resistant technologies;[4] Next Generation 911,[5] including Text-to-911;[6] persistent airborne surveillance;[7] laser spectroscopy devices, and vehicle pursuit darts.[8] These technologies and others are notable, but the field of technology as it relates to law enforcement is large and dynamic, and the implications for the different types of technologies cannot be covered in detail.

To assist agencies in determining whether they should implement a new technology or data-enabled capability, the commission's working group considered and tested two frameworks: one for adopting new technologies, and one for the handling and use of data. Each 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. These evaluations offer law enforcement executives the flexibility to address specific issues in their unique circumstances, and they will evolve over time as law enforcement faces challenges and opportunities and as new technologies become available for use by law enforcement or are used by criminals to counter law enforcement objectives. These frameworks draw upon others, such as the International Association of Chiefs of Police (IACP) Technology Policy Framework. As Commissioner Chris Evans, the Chief of Operations at the Drug Enforcement Administration, stated, "The [process for using the frameworks] is flexible and will help agencies over time."[9] Through the work of law enforcement executives, personnel, and the potential engagement of the National Domestic Communications Assistance Center (NDCAC), the frameworks can help steer law enforcement in the right direction during their technology acquisition and data management process.

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 data set or the adoption of a new technology. These tools can guide law enforcement executives through decision-making processes, assessing the pros, cons, and other predictable considerations, but they are not intended as a checklist where all questions must be answered each time. Rather, only the applicable questions should be considered for a particular technology or data set.

For example, the question may be raised, how can agencies ensure the use of the technology is not perceived as overly intrusive? Potential answers include training, communications with the public, and limiting the technology's use through technical methods or audits.

The commission has opted to address certain themes that transcend the deployment of technologies or acquisition of data sets while highlighting some of the most common technological challenges faced by law enforcement agencies today. As stated by David Bowdich, the Deputy Director at the Federal Bureau of Investigation (FBI), "We need to think about [the implications of technology] years down the road."[10] From the technology adoption phase to the implementation and maintenance phase, the frameworks were developed to inform the way in which agencies make technology and data-related decisions.

---

[4] Donald Washington, Director, United States Marshals Service, in discussion with Joe Heaps, Federal Program Manager, Technology Working Group, February 28, 2020.

[5] Dean Kueter, Executive Director, President's Commission on Law Enforcement and the Administration of Justice, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, February 24, 2020.

[6] Theophani K. Stamos, Office of Executive Director, President's Commission on Law Enforcement and the Administration of Justice, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 16, 2020.

[7] Theophani K. Stamos, Office of Executive Director, President's Commission on Law Enforcement and the Administration of Justice, email Communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 4, 2020.

[8] Phil Keith, Director, COPS Office, email communication with Rob Chapman, Deputy Director, COPS Office, April 3, 2020.

[9] D. Christopher Evans, Chief of Operations, Drug Enforcement Administration, in discussion with Technology Working Group, virtual meeting, March 6, 2020.

[10] David Bowdich, Deputy Director, Federal Bureau of Investigation, in discussion with Technology Working Group, virtual meeting, February 21, 2020.

## 6.1 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."[11] - 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. Darrin Jones, the Executive Assistant Director for Science and Technology at the FBI, notes that a growing number of U.S. tech companies have 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.[12] [13] 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.

### 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."[14] - 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 lawful access of otherwise accessible, court-authorized information becomes restricted. While most publicized instances of this relate to the FBI and terrorism, state and local police departments encounter these types of encryption issues 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 local police departments cannot gain lawful access to critical criminal evidence that has been encrypted, they will

---

[11] *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*, (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.

[12] Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation, President's Commission on Law Enforcement and the Administration of Justice, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, June 10, 2020.

[13] Oded Gal, "The Facts Around Zoom and Encryption for Meetings/Webinars," *Zoom Blog* (blog), April 1, 2020, https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/. During the Technology Working Group's proceedings, a major online video-conferencing provider made popular by the COVID-19 pandemic, Zoom, announced a change in its security policies. On April 1, 2020, Zoom 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;" Eric S. Yuan, "Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering," *Zoom Blog* (blog), 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/, May 7, 2020. On May 7, 2020, Zoom issued a stronger anti-law enforcement public statement following their acquisition of Keybase, announcing 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." (Emphasis added.)

[14] *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*, (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.

have to turn for assistance to larger federal agencies whose own resources are already taxed. As a result, federal agencies may decide which state and local crimes are investigated and prosecuted, regardless of the priorities of state and local officials.

In March 2019, Facebook announced its intention to encrypt Facebook Messenger.[15] 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.[16] While the commission recognizes and applauds Facebook's substantial efforts to combat these 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."[18] – 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 identified 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. Moreover, 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.

The New York district attorney's office 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.[19] 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. In doing so, these companies upended more than 200 years of jurisprudence by placing evidence beyond the reach of a court-ordered search warrant. Through this action, private companies weakened the justice system and handicapped law enforcement's ability to protect

---

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

[16] Rt Hon Priti Patel MP, United Kingdom Secretary of State for the Home Department; William P. Barr, United States Attorney General; Kevin K. McAleenan, United States Secretary of Homeland Security (Acting); and Hon Peter Dutton MP, Australian Minister for Home Affairs in letter to Mark Zuckerberg, Chief Executive Officer, Facebook, Inc., *Open Letter: Facebook's "Privacy First" Proposals,* October 4, 2019, *https://www.justice.gov/opa/press-release/file/1207081/download*.

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

[18] Clark, *President's Commission on Law,* May 4, 2020.

[19] *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* (April 15, 2020) (written statement of Cyrus R. Vance Jr., District Attorney, New York County, New York), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

and promote the public's safety.

**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, ensuring lawful access to evidence pursuant to court orders, and should preclude immunity from liability for these same providers who fail to do so.**

**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."[20] – Darrin Jones, Executive Assistant Director for Science and Technology, Federal Bureau of Investigation

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.[21] 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 decades of candid discussions initiated by law enforcement with a number of these providers and manufacturers, the companies have made little progress to resolve these lawful access issues voluntarily. Instead, during that period, the problem has worsened and threatens to become the norm.

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 without justice.

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 that 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.[22]

---

[20] *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* (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.

[21] "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 et seq. (2006), https://www.law.cornell.edu/uscode/text/47/1001.

[22] International Association of Chiefs of Police, *IACP 2019 Resolutions Adopted* (Alexandria, VA: International Association of Chiefs of Police, 2019), 45-46, https://www.theiacp.org/sites/default/files/Adopted%202019%20Resolutions__Final.pdf. The paragraph refers to Resolution 21 of the IACP December 2019 Resolutions.

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 in determine whether to dedicate resources to harm−mitigation strategies—may not influence some of these technology companies into a willingness to facilitate lawful access.

So 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.

## 6.2 Lawful Access Technology Resource Center

### Background

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: "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, "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."[23]

Kevin Jinks, the Senior Counsel from the Office of Legal Policy at the Department of Justice, expanded upon Dr. Vorder Bruegge's comments by identifying two questions agencies should consider during the technology acquisition process:

- Will the requirement owner be able to reuse this tool for a different purpose in the future?
- How will this tool work with other tools (e.g., one shared user interface for a radar, camera, and RF-based technology)?[24]

**[CROSS REFERENCE REDUCTION IN CRIME; HOMELAND SECURITY]**

The pace of both the evolution and iteration of technologies can potentially both assist and challenge law enforcement. However, few police departments have the resources to keep abreast of this evolution on an ongoing basis. Law enforcement agencies need an enduring, shared, collaborative structure that can serve as a hub for technical knowledge management, facilitate the sharing of solutions and knowledge among law enforcement agencies, and inform and strengthen law enforcement's relationships with the communications industry.

---

[23] *President's Commission on Law Enforcement and the Administration of Justice: Reduction of Crime Hearing Technology Tools Panel* (April 21, 2020) (statement of Erica MacDonald, Commissioner), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings; *President's Commission on Law Enforcement and the Administration of Justice: Reduction of Crime Hearing Technology Tools Panel* (April 21, 2020) (statement of Dr. Richard Vorder Bruegge, Senior Physical Scientist, Federal Bureau of Investigation), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

[24] Kevin Jinks, Senior Counsel from the Office of Legal Policy at the Department of Justice, email communication with Joe Heaps, Federal Program Manager, Technology, April 21, 2020.

## Current State of the Issue

Established by the FBI, the National Domestic Communications Assistance Center (NDCAC) opened in 2013 to help federal, state, local, tribal, and territorial law enforcement to keep abreast of the communications revolution.[25] Located in Fredericksburg, Virginia, 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. Therefore, to a limited extent, the NDCAC already serves as a hub for technical knowledge management, facilitates the sharing of solutions and knowledge among law enforcement agencies, and informs and strengthens law enforcement's relationships with the communication industry.

Since its establishment, the NDCAC has grown in importance to the law enforcement community, assisting a multitude of law enforcement officers, answering queries, and providing training to students.[26] The Intelligence Commanders Group (ICG) of the Major Cities Chiefs Association (MCCA) and Major County Sheriffs of America (MCSA) recognize that the NDCAC "is a tremendously valuable resource, [because] it is not practical or possible for every one of the thousands of state and local law enforcement agencies across the country to have, within their own department, adequate access to resources and expertise."[27] However, as currently structured, the NDCAC focuses almost exclusively on issues involving real-time lawful interception and the recovery of stored communications.

NDCAC engineers help test industry-developed lawful intercept technical solutions that claim to comply with the CALEA,[28] and they provide substantive technical input and closely monitor the work of groups that set industry standards as they relate to lawful access issues. The NDCAC also operates a nationwide assistance center available to verified law enforcement officers who investigate the nation's most serious crimes.[29] Funding permitting, the NDCAC also offers periodic technology and digital forensic training sessions to state and local officers. 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.

### 6.2.1 The Federal Bureau of Investigation should restructure the National Domestic Communications Assistance Center's Executive Advisory Board to allow law enforcement executives from federal, state, local, tribal, and territorial law enforcement agencies to address specific and sensitive law enforcement matters, including the impact and development of emerging technologies on law enforcement operations.

Currently, an Executive Advisory Board (EAB) of approximately 15 members who represent a wide range of law enforcement agencies assists the NDCAC in its mission. The EAB provides some measure of state and local insight to inform the vision of the NDCAC; however, its current structure limits law enforcement's ability to candidly discuss sensitive operational information relating to ongoing investigations that involve technology requirements and objectives and their gaps, limitations, and vulnerabilities.

---

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

[26] National Domestic Communications Assistance Center, "May 2017 EAB Meeting Minutes," September 29, 2017, https://ndcac.fbi.gov/file-repository/may2017eabmeetingminutes.pdf/view.

[27] Laura Cooper, Executive Director, Major Cities Chiefs Association, email communication with President's Commission on Law Enforcement and the Administration, April 29, 2020; Major Cities Chiefs Association, *Critical Issues for Intelligence Commanders* (Washington, DC: National Domestic Communications Assistance Center, 2018), 43, https://ndcac.fbi.gov/file-repository/mcca-intelligence-commander-group-critical-issues-series -final.pdf/view.

[28] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001 (1994), *et seq.* https://www.law.cornell.edu/uscode/text/47/2. CALEA requires that a defined class of telecommunications carriers develop lawful interception solutions which they control but which may be activated by the carriers when they are presented with a lawful order, such as court wiretap order issued after a finding of probable cause by a judge. CALEA has historically applied primarily to traditional telecommunications companies operating landline, cellular or mobile, and cable-based telephone technology. CALEA has not yet been found to explicitly apply to software-only-based application providers whose services generally do not manage communications connecting to the public-switched telephone network.

[29] The NDCAC's Law Enforcement Assistance Center is managed by the Technology Resources Group. Email inquiries can be sent to: AskNDCAC@fbi.gov.

The EAB board should be restructured in a manner that encourages and ensures an environment where law enforcement executives may freely collaborate over their shared needs. Restructuring the EAB would also allow it to take on a broader role in identifying the most important technologies affecting law enforcement, local prosecutors, and their communities. The restructured EAB should also identify research, training, tools, frameworks, and other technologies that could help state and local law enforcement agencies deal with emerging technologies. Further, the EAB should help all law enforcement agencies—large, small, urban, and rural—identify and prioritize the impacts, challenges, opportunities, gaps, and requirements of operating and managing technology.

**6.2.2 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. This should include technologies that may affect law enforcement investigations and operations. 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.

In addition, the NDCAC previously published an *Emerging Technology Review Bulletin* (*ETR Bulletin*) in a similar format to the *FBI's Law Enforcement Bulletin*.[30] The *ETR Bulletin* was a compendium of plain language explanations of emerging technologies and their potential or actual impact on law enforcement. The NDCAC should consider reviving this publication and distributing it through traditional print and digital format on its online repository and disseminating it across law enforcement agencies. The *ETR Bulletin* should serve as a complementary, semi-annual compendium of the NDCAC's most significant research.

**6.2.3 The National Domestic Communications Assistance Center should provide broad, inexpensive, and easily accessible training to federal, state, local, tribal, and territorial 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 offers state and local officers periodic technology and digital forensic training sessions on a limited basis. The NDCAC's training efforts have been recognized within and outside of the law enforcement community. The Center for Strategic and International Studies (CSIS) highlights potential solutions to law enforcement's challenges with digital evidence, recommending, "Congress can and should adequately resource NDCAC to serve the training and technical roles that already fall within its mission."[31]

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. It should also explore new ways to deliver 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 others expanding on technological issues and challenges.[32]

---

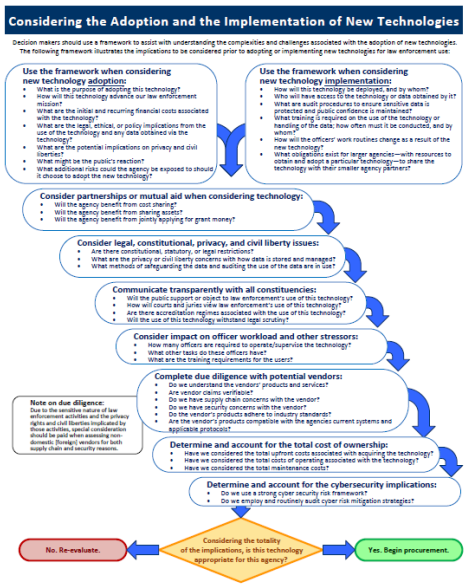
[30] "FBI Law Enforcement Bulletin," Federal Bureau of Investigations, December 1, 2012, https://leb.fbi.gov/bulletin-highlights/additional-highlights/fbi-law-enforcement-bulletin-a-history.

[31] William A. Carter, Jennifer C. Daskal, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, (Washington, DC: Center for Strategic and International Studies (CSIS), 2018), https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.

[32] The prioritized access of "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.

## 6.3 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)[33]




Source: Executive Office of the President of the United States, Report of the President's Commission on Law Enforcement and the Administration of Justice, Technology Working Group

## Background

Law enforcement has relied on technology and resources to augment their roles since the 1830s, when multi-shot pistols were implemented in police agencies nationwide.[34] Fingerprinting was introduced in the 1900s, and crime laboratories were introduced in the 1920s. These advancements greatly enhanced law enforcement's efforts to solve crimes. The invention of the two-way radio and the surge in automobile use in the 1930s bolstered law enforcement's productivity by increasing their incident response numbers.[35] One of the most monumental technologies in the history of law enforcement is the 911-call system, which was invented after the Johnson commission.[36] From the creation of soft body armor in 1972 to the emergence of crime mapping computer programs in the 1990s, technology has been interwoven into how policing is conducted.

Law enforcement agencies are inundated with news of innovative technologies and advancements. Sifting through what could be useful to the agency is no easy task, and acquisition and implementation adds another layer of complexity—not to mention significant costs in the face of budgetary constraints. Deployment of

---

[33] Robert J. Tracy, Chief of Police, Wilmington, DE, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 20, 2020.

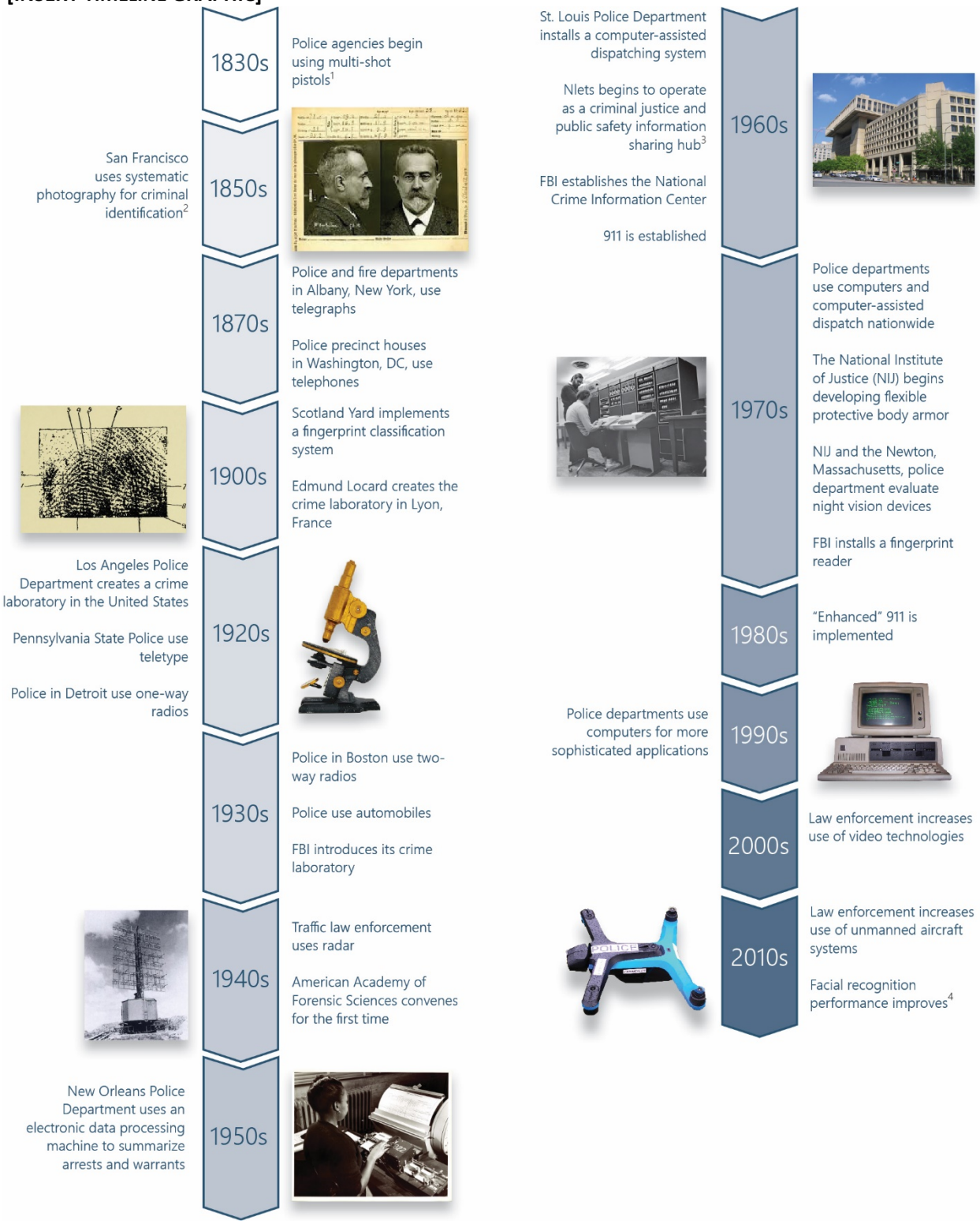
[34] "Samuel Colt," History.com, last modified January 30, 2019, https://www.history.com/topics/inventions/samuel-colt; SeaSkate, Inc., *The Evolution and Development of Police Technology* (Washington, DC: The National Committee on Criminal Justice Technology, 1998), https://www.justnet.org/pdf/PoliceTech.pdf .

[35] SeaSkate, *The Evolution and Development of Police Technology*.

[36] SeaSkate, *The Evolution and Development of Police Technology*.

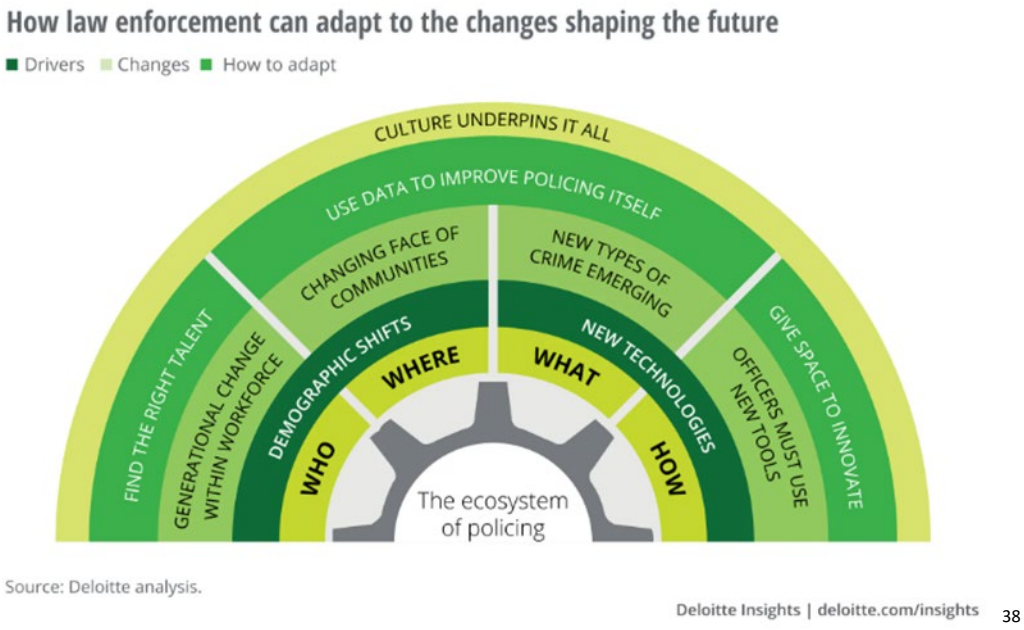
new technologies may also raise other issues for consideration, including public acceptance and Constitutional and legal concerns.

**[INSERT TIMELINE GRAPHIC]**



Current State of the Issue

While the law enforcement field has welcomed a younger, more digitally savvy workforce in recent years, agencies may still lack the necessary resources to make fully informed and prudent decisions regarding the adoption of emerging technologies, and to properly evaluate their short- and long-range implications if adopted.[37]




Source: Deloitte: https://www2.deloitte.com/us/en/insights/focus/defense-national-security/future-of-law-enforcement-ecosystem-of-policing.html

The National Institute of Justice (NIJ) provided funding to RTI International and the Police Executive Research Forum (PERF) in 2012 to review the various technologies that law enforcement agencies purchased and used.[39] The study, published in 2016, found that out of the more than 1,200 state and local law enforcement agencies surveyed, 96 percent had adopted at least one of the 18 main technologies listed in the survey:

- 70 percent used in-car cameras
- 68 percent used platforms that facilitate the transfer of information
- 68 percent used social media

In addition, a third of agencies used

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

---

[37] *President's Commission on Law Enforcement and the Administration of Justice: Hearings on Rural and Tribal Challenges Law Enforcement Face in Rural Areas*, (May 19, 2020) (written statement of Michael A. Keller, Andover Chief of Police, City of Andover, KS), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

[38] Dr. Michael Gelles, Alex Mirkow, and Joe Mariani, *"*The Future of Law Enforcement: Policing Strategies to Meet the Challenges of Evolving Technology and a Changing World*," Deloitte Insights*, October 22, 2019, https://www2.deloitte.com/us/en/insights/focus/defense-national-security/future-of-law-enforcement-ecosystem-of-policing.html.

[39] Kevin Strom, *Research on the Impact of Technology on Policing Strategy in the 21st Century* (Washington, DC: National Institute of Justice, 2016), https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf.

- software to investigate and manage cases

There was a pattern among agencies with 250 or more officers of using technology with analytical and visual features.[40]

The study also indicated that the technology in many agencies was not always acquired methodically, but was often purchased and implemented on an "ad hoc" basis. For many agencies, "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 disillusionment and a lack of continuation funding for maintaining or updating particular types of technology."[41]

The study emphasized the need for law enforcement agencies to

- make decisions on new technology by using evidence-based research
- implement new technologies in a strategic manner
- increase collaboration among technology experts and agency leadership

6.3.1 **Law enforcement agencies should employ consistent and comprehensive analysis when considering the adoption of new technologies.**

The case in which a combination of technologies was used to catch a murderer illustrates the importance of technology in law enforcement (see text box). To assess the benefits, risks, and costs 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 costs and risks. Not all elements of the framework may be needed to address each technology. Additionally, the framework should be periodically refreshed to ensure it accommodates newly identified risks or benefits posed from changes in mission or law, the emerging technologies, or public perception.

Historically, agencies have often considered the adoption of a technology first, and then considered how to implement it efficiently within their organization. When law enforcement learns of a new technology, the operational benefits of deploying that technology may be immediately apparent. What may be less apparent are the back-end risks or cost associated with deploying the technology. Additionally, information obtained during the technology adoption phase may inform the direction of the technology implementation phase.

Questions during the adoption phase may include:

- What is the purpose of adopting this technology?
- How will this technology advance our law enforcement mission?
- What are the initial and recurring financial costs?
- What are the legal, ethical, or policy implications of using the technology and any data obtained from it?
- 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 if it adopts the technology?

**6.3.2 Law enforcement agencies should thoroughly research and consider the full range of policy, legal, constitutional, and ethical implications. 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**

[40] Strom, *Research on the Impact of Technology*.
[41] Strom, *Research on the Impact of Technology*.

**appropriate, that are associated with adopting new technology.**

When implementing new technology, agencies must consider its legal and policy implications, including any affirmative authorizations required or constraints imposed, as well as any impact on privacy rights and civil liberties. In addition to Fourth Amendment warrant requirements, there may also be statutory limitations on the acquisition and use of various types of information. In *City of Ontario, California, et al.* v. *Jeff Quon, et al*.,[42] a case involving an employer-provided pager, the Supreme Court decided the case on a narrow question and did not consider the far-reaching issues raised on the grounds that modern technology and its role in society was still evolving. Supreme Court cases like *United States* v. *Jones* (involving tracking devices)[43] and *Timothy Ivory Carpenter* v. *United States* (involving location information)[44] provide insight to the court's assessment of the evolving nature of technology and its implications on constitutionally protected individual privacy interests.

The Supreme Judicial Court of Massachusetts recently held in *Commonwealth of Massachusetts* v. *Jason J. McCarthy* 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 the defendant's constitutional rights.[45]

Groups who may be affected by the implementation of a new technology could include the general public, elected officials, local advocacy groups, and law enforcement labor organizations. In addition, partners such as the American Civil Liberties Association (ACLU) may wish to provide input, which can enhance public acceptance of law enforcement's use of a specific technology.

**[BEGIN TEXT BOX]**

**Bird's Eye View: Using Unmanned Aircraft Systems (UAS) Technology**

One evening in August 2017, a Wilmington (Delaware) Police Department officer 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.[46]

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 certainly put officers at risk should the suspect have been present, and so the team deployed a drone equipped with an on-board thermal imaging camera, which was able to show that the movement was coming 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. – Chief Robert Tracy, Chief of the Wilmington, Delaware police department[47]

**[END TEXT BOX]**

**6.3.3 Before adopting a new technology, law enforcement agencies should assess the overall impact to the agency and its personnel.**

---

[42] Ontario v. Quon, 560 U.S. 746 (2008), https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf .
[43] US v. Jones, 565 U.S. 400 (2012), https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.
[44] Carpenter v. US, 585 U.S. 138 S. Ct. 2206 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.
[45] Commonwealth v. McCarthy, 385 Mass. 160 (1982), https://socialaw.com/services/slip-opinions/slip-opinion-details/commonwealth-vs.-jason-j.-mccarthy.
[46] Robert Tracy, Chief, Wilmington, DE, Police Department, email communication with Josephine Debrah, Report Writer, and Joe Heaps, Federal Program Manager, Technology Working Group, April 1, 2020.
[47] Tracy, Technology Working Group, April 1, 2020.

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 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 with the de-escalation of events. As evidenced by the CVPD's experience with UAS, introducing the technology directly supported the officers' ability to de-escalate otherwise difficult response efforts.[48] The CVPD also uses drones to respond to 911 calls, with the UAS response time being under three minutes. [49] The CVPD works closely with the Federal Aviation Administration (FAA) as part of the FAA UAS Integration Pilot Program (IPP).[50] During a recent period, the CVPD states the UAS teleoperators[51] were able to clear more than 15 percent of calls without requiring ground unit response.[52]

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

**6.3.4 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 adhere to professional standards and accreditation programs when selecting products and services.**

Emerging technologies are entering the market place rapidly. It is incumbent upon law enforcement agencies to research the vendors, as well as the products and services they are considering. 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 verify the accuracy of the vendor's statements and data. Due to the sensitive nature of law enforcement activities, privacy issues and civil liberties potentially impacted by the technology should be considered, particularly when assessing 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 being considered. 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 discovering prior efforts to vet vendors and could lead to time and cost savings.[53] 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. For example, the evolution of Rapid DNA technology illustrates how technology designed for the rapid analysis of DNA, taken from a single source, could be erroneously used to analyze DNA from a much less discrete 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

---

[48] 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/.

[49] "HigherGround," www.higherground.com, accessed June 1, 2020; "UAS Drone Program," Chula Vista Police Department (CVPD), accessed June 1, 2020, https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program; Vern Sallee, Patrol Operations Division Captain, Chula Vista Police Department, email communication with Joe Heaps, Federal Program Manager, Technology, June 9, 2020.

[50] Federal Aviation Administration, "Fact Sheet – The UAS Integration Pilot Program," March 31, 2020, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=23574.

[51] "HigherGround," www.higherground.com, accessed June 1, 2020; "UAS Drone Program," Chula Vista Police Department (CVPD), accessed June 1, 2020, https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program; Vern Sallee, Patrol Operations Division Captain, Chula Vista Police Department, email communication with Joe Heaps, Federal Program Manager, Technology, June 9, 2020.

[52] Verne Sallee,"Drone as a First Responder."

[53] Al Cannon, Sheriff, Charleston County, SC, Technology Working Group Member, in discussion with Joe Heaps, Federal Program Manager, Technology Working Group, February 28, 2020.

quickly, at present, Rapid DNA instruments and collection protocols are not sufficiently mature for use in analyzing crime scene evidence. **[CROSS-REFERENCE RECRUITMENT, RETENTION, AND TRAINING]**

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

The total cost of ownership of new technology includes not only the upfront costs associated with acquiring the technology but also the operations and maintenance costs. Consideration must be given to the storage of any data generated, as well as expenses for training, certification, intellectual property licenses, or online access fees.

An example of an 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 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.[54] 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, Delaware 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. [55]

**[CROSS REFERENCE REDUCTION IN CRIME]**

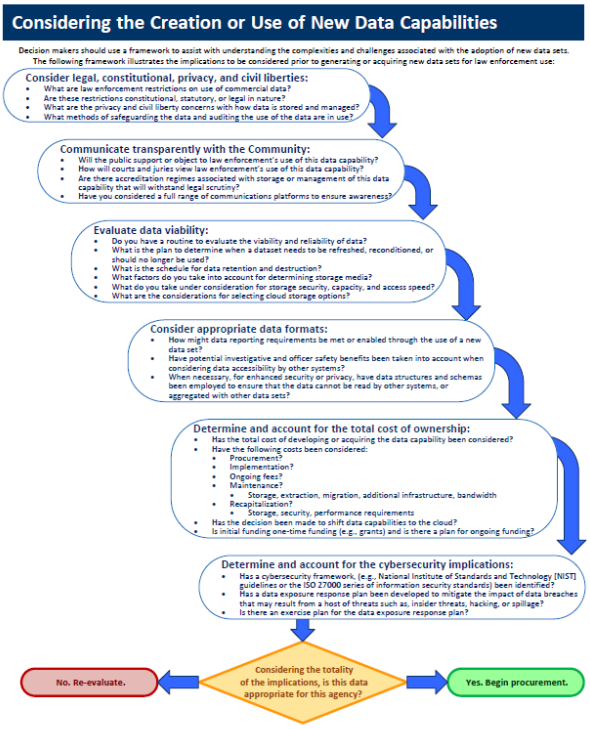
**6.3.6 Law enforcement agencies should apply cybersecurity frameworks when implementing technologies that are supported by digital or cyber components.**

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 require strong cybersecurity risk frameworks. Agencies must diligently employ and routinely audit their mitigation strategies to ensure effective implementation and actual risk reduction.

[54] Jillian Carr and Jennifer L. Doleac, "The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data," *SSRN* (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770506.

[55] Chief Robert Tracy, Wilmington, DE, Police Department, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, May 15, 2020.

## 6.4 Creating and Using New Data Capabilities




Source: Executive Office of the President of the United States, Report of the President's Commission on Law Enforcement and the Administration of Justice, Technology Working Group

### 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. 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" mentioned previously, the "data framework" must be general enough to be applicable across a broad range of data types, yet specific enough to help 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 of whether the new data set is to be generated anew internally to the law enforcement organization, acquired externally from commercial or other partners, or created through the aggregation of different internal or external data sets. Agencies should also routinely refresh and reengage their frameworks 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 have 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 degree, generating and accumulating 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. The generation and 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 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.[56]

**[CROSS REFERENCE INTERSECTION OF CRIMINAL JUSTICE PERSONNEL]**

### 6.4.1 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 data set.

Within the last few years, the volume of third-party data available for resale to public and private entities has grown exponentially.[57] 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 that data is obtained or used 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.[58]

### 6.4.2 Law enforcement agencies generating, acquiring, or using new data sets should openly communicate with the community to ensure the community clearly understands the new data set, its use, and what protections are in place.

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 data set for a particular law enforcement purpose (by considering, e.g., public expectations of the propriety nature of the data, safety, privacy, and protection of civil liberties). Additionally, agencies must consider how courts and juries may view law enforcement's use of any new data set. 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 data set, if they can withstand legal scrutiny, or if there are any legal implications to not using such regimes.

### 6.4.3 Law enforcement agencies should 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.[59] As new data analytics technologies continue to evolve, highly proprietary or otherwise

---

[56] *President's Commission on Law Enforcement and the Administration of Justice: Hearing on Crime Reduction – Domestic Violence and Sexual Assault, Technology Issues Encountered by Law Enforcement, Leveraging Technology to Reduce Crime (April 16, 2020*) (written statement of Thomas Ruocco, Division Chief, Criminal Investigations Division, Texas Department of Public Safety, Austin, TX), https://www.justice.gov/ag/presidential-commission-law-enforcement-and-administration-justice/hearings.

[57] Max Freedman, "How Businesses Are Collecting Data."

Carpenter v. US, 585 U.S. 138 S. Ct. 2206 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

[59] Hollywood and Winkelman, *Improving Information-Sharing,* 3.

unique in-house storage arrangements may limit the ongoing or future use of a data set. Similarly, data sharing among law enforcement agencies can have enormous investigative and officer safety benefits, but 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 data sets, in an effort to enhance security or privacy or better protect civil liberties.

**[CROSS REFERENCE OFFICER HEALTH AND WELLNESS AND INTERSECTION OF CRIMINAL JUSTICE PERSONNEL]**

**6.4.4 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.[60] This total cost includes all expenses 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 recurring expenses of maintaining and refreshing systems (e.g., storage, extraction and migration, additional infrastructure, bandwidth, security, and performance requirements).

As technology and data capabilities continually improve and evolve, so does the requirement to ensure systems and data sets 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.

## 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."[61] – 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.[62] The technology to compare two images using a computer algorithm has been in

[60] Hollywood and Winkelman, *Improving Information-Sharing,* 18.
[61] BJay Pak, United States Attorney Northern District of Georgia, email communication with Joe Heaps, Federal Program Manager, Technology Working Group, April 30, 2020.
[62] Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," Abstract, *Minnesota Law Review, Vol. 105 forthcoming*, (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423.

development for nearly 40 years.[63] It works by creating a digital "face print" of a subject and seeks to match the print to a known image of a person:[64]

> 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 data sets 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.[65]

Since the 1960s, facial recognition technology has continued to evolve, and "progress was steady, but slow, until the recent arrival of advanced artificial neural networks (e.g. computer systems)."[66] When combined with a system of cameras, FRT can help law enforcement investigate crimes, reduce the pool of persons of interest and suspects, exonerate the innocent, and maximize 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 in the future. At the same time, law enforcement should be transparent about its use 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.[67] 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.[68] Custodial and supervisory use includes using FRT as a form of biometric identification throughout the criminal justice process.[69] Investigative use includes applying FRT to surveillance footage or other photographs to identify potential suspects, associates, witnesses, or victims for investigative leads.[70]

The New York Police Department has used FRT to generate leads for persons of interest since 2011.[71] The FBI operates two FRT programs: the Next Generation Identification Interstate Photo System and the Face Analysis, Comparison, and Evaluation Service program.[72] Facial recognition programs provide information that is not readily available with the use of other methods of investigation. The FBI states, "more than 6,000 face recognition leads have been returned to FBI agents and other investigators. Most investigations are

---

[63] 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 (available at SSRN ID 330512).

[64] 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.

[65] Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment," *Minnesota Law Review*, Vol. 105 forthcoming, (2019): 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423.

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

[67] Law Enforcement Imaging Technology Task Force, *Law Enforcement Facial Recognition Use Case Catalog,* (Alexandria, VA: International Association of Chiefs of Police (IACP), 2019): 7, https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf.

[68] Law Enforcement Imaging Technology Task Force, *Law Enforcement Facial Recognition,*" 8-10.

[69] Law Enforcement Imaging Technology Task Force, *Law Enforcement Facial Recognition,*" 15-17.

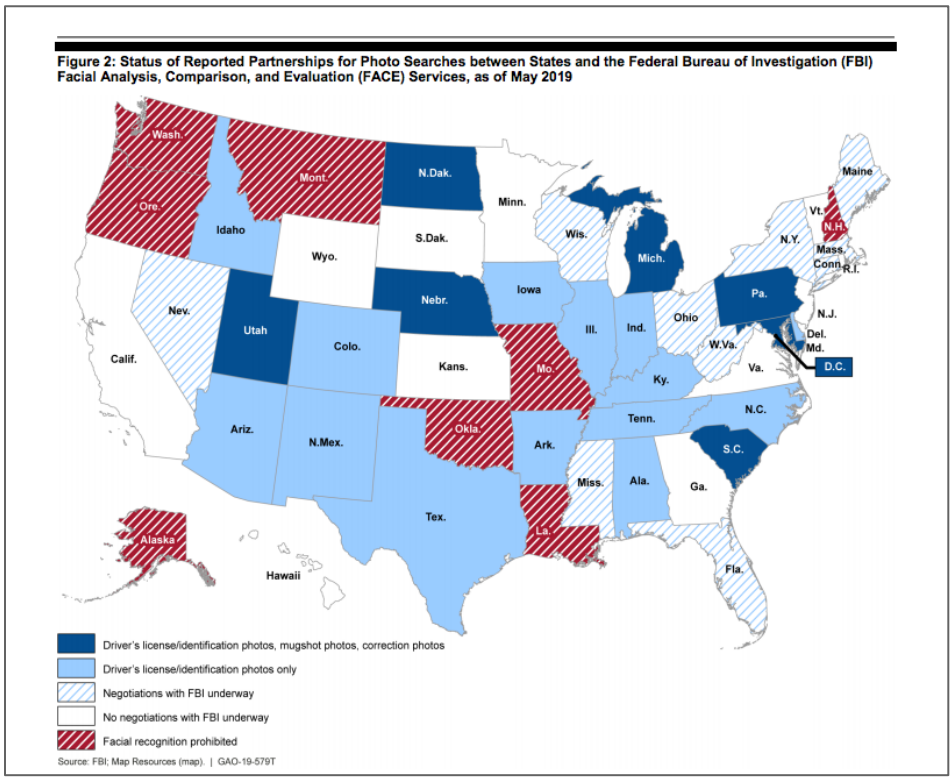
[70] *House of Representatives Committee on Oversight and Reform: Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains* (June 4, 2019) (statement of Gretta L. Goodwin, Director, Homeland Security and Justice), https://www.gao.gov/assets/700/699489.pdf.

[71] Brown, "There Will Be No Turning Back."

[72] "Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit," Federal Bureau of Investigation, May 1, 2015, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit; "Next Generation Identification (NGI)," Federal Bureau of Investigation, accessed July 6, 2020, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

ongoing, but two arrests have been made as a result of leads provided by the FACE Services Unit, and two victims from a violent crimes case have been located." [73]

Kimberly J. Del Greco, Deputy Assistant Director of the FBI's CJIS Division, stated, "from fiscal year 2017 through April 2019, the FBI's CJIS Division received 152,565 facial recognition search requests of the Next Generation Identification Interstate Photo System (NGI-IPS) repository from authorized law enforcement users. During that time, there have been no findings of civil liberties violations or evidence of system misuse."[74]




Source: FACE RECOGNITION TECHNOLOGY: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains GAO-19-579T: Published: Jun 4, 2019. Publicly Released: Jun 4, 2019.

Concerns about FRT can be grouped into three areas: privacy and civil liberties concerns, data security and hacking concerns, 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.[75]

Entities collect a large number of photos of the public, at times without their knowledge or consent. People also voluntarily provide photos to commercial entities (e.g., social media companies) whose terms of service

---

[73] *House Committee on Oversight and Reform: Facial Recognition Technology, Part II: Ensuring Transparency in Government Use,* (June 4, 2019) (statement of Gretta L. Goodwin, Director, Homeland Security and Justice ), https://www.gao.gov/assets/700/699489.pdf.

[74] U.S. *House Oversight and Reform Committee: Facial Recognition Technology: Ensuring Transparency in Government Use* (June 4, 2019) (statement of Kimberly J. Del Greco Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use.

[75] *U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law: What Facial Recognition Technology Means for Privacy and Civil Liberties* (August 23, 2012), (written statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), https://www.judiciary.senate.gov/imo/media/doc/12-7-18LynchTestimony.pdf; Ashley Deeks and Shannon Togawa Mercer, "Facial Recognition Software: Costs and Benefits," *Lawfare* (blog), March 27, 2018, https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits.

allow 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 location. Such tracking may infringe on an individual's First Amendment rights to free speech and association, and the Fourth Amendment rights against unreasonable searches and seizures.[76]

Additionally, there is concern that "face scanners used to unlock [a] smartphone or other devices aren't nearly as secure as they're made out to be."[77] 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.[78]

**[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.[79] These organizations recommend that the law enforcement agencies

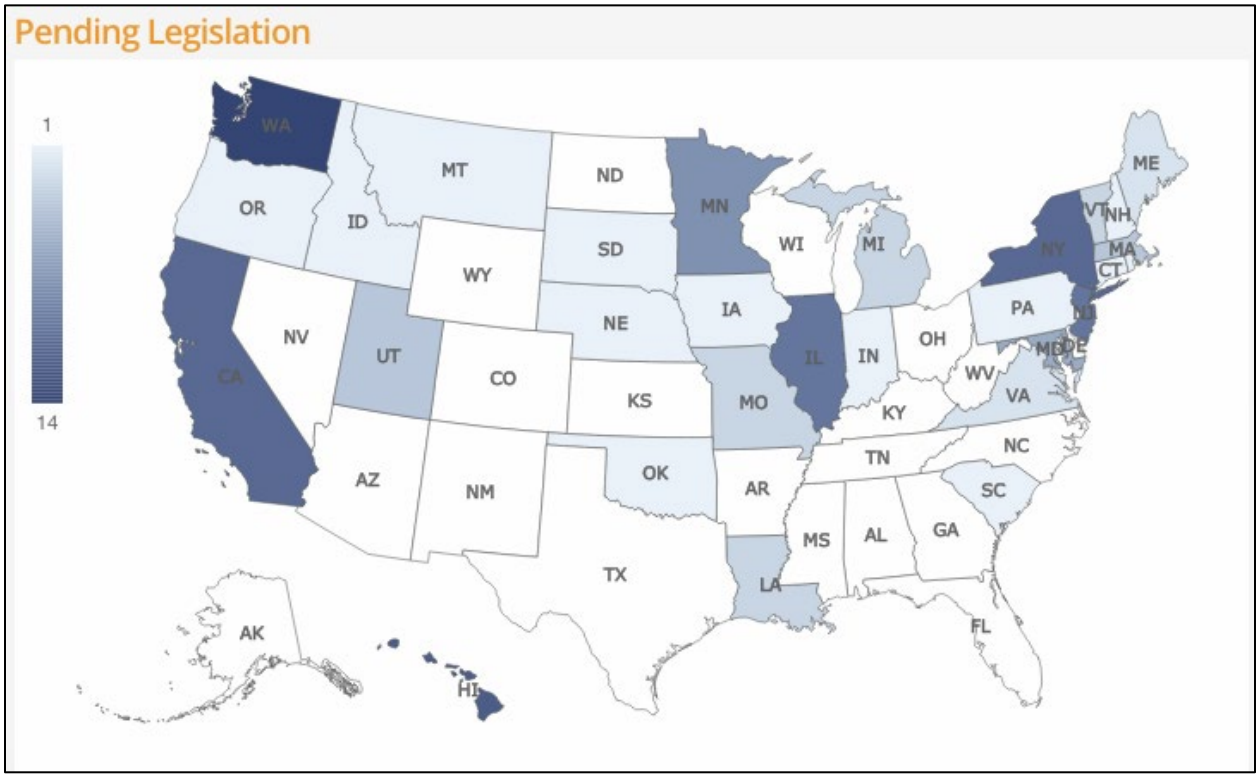
- provide complete information to the public on how and when FRT is used, and how it is collected and stored
- establish parameters of use to engender public confidence
- publicize the effectiveness of FRT by citing real-life success stories
- develop principles and policies for best practice[80] adhere to laws and governmental policies in their jurisdiction[81]
- ensure protection of constitutional rights of individuals
- use facial recognition as a part of an investigation, not "the basis for any law enforcement action"[82]
- require training on all facets of the technology for all users[83]

**[END TEXT BOX]**

Some jurisdictions have rushed to pass laws or ordinances that significantly limit the use of FRT by law enforcement agencies. In May 2019, San Francisco, California, banned the use of FRT by law enforcement

[76] Lynch, "What Facial Recognition Technology Means," 5.
[77] Wengchang Yang and Song Wang, "Finger and Face Scanners Aren't as Secure as We Think They Are," Government Technology, March 6, 2019, https://www.govtech.com/security/Finger-and-Face-Scanners-Arent-as-Secure-as-We-Think-They-Are.html;
Brown, "There Will Be No Turning Back."
[77] Federal Bureau of Investigation, "Next Generation Identification (NGI)."
[78] Brown, "There Will Be No Turning Back**."**
[79] Law Enforcement Imaging Technology Task Force, *Law Enforcement Facial Recognition.*
[80] Law Enforcement Imaging Technology Task Force, *Law Enforcement Facial Recognition,* 17–19.
[81] https://www.theiacp.org/resources/document/guiding-principles-for-law-enforcements-use-of-facial-recognition-technology
[82] https://www.theiacp.org/resources/document/guiding-principles-for-law-enforcements-use-of-facial-recognition-technology
[83] https://www.theiacp.org/resources/document/guiding-principles-for-law-enforcements-use-of-facial-recognition-technology

agencies.[84] In addition, Oregon,[85] New Hampshire,[86] California,[87] and Washington[88] have statutes that limit the use of FRT.




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.[89] Federal agencies, such as the FBI, have already adopted a set of policies to ensure appropriate use of FRT.[90] The following are key elements of the FBI's policy:

---

[84] Rachel Metz, "Beyond San Francisco, more cities are saying no to facial recognition," CNN Business, July 17, 2019, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[85] Or. Rev. Stat. § 133.741 (2020), Law enforcement agency policies and procedures regarding video and audio recordings, https://www.oregonlaws.org/ors/133.741.

[86] N.H. Rev. Stat. § 263:40-b (2015), https://law.justia.com/codes/new-hampshire/2015/title-xxi/chapter-263/section-263-40-b/. Use of Facial Recognition Technology Prohibited: (2015) N.H. Rev. Stat. § 263:40-b (2015) (prohibiting the state department of motor vehicles from using FRT); N.H. Rev. Stat. § 260:14 (prohibiting the department of motor vehicles from sharing driver's license photographs with the federal government); and N.H. Rev. Stat. § 105-D:2 XII (prohibiting use of FRT on body worn camera footage).

[87] Cal. Pen. Code § 832.19 (2020), Law enforcement: facial recognition and other biometric surveillance, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215, Matt O'Brien, "Why some cities, states and lawmakers want to curb facial recognition technology," Associated Press, December 17, 2019, https://www.usatoday.com/story/tech/2019/12/17/face-recognition-ban-some-cities-states-and-lawmakers-push-one/2680483001/.

[88] H. S.B. 6280, 66th Leg., 2020 Sess. §1(1) (Wash. 2020), Concerning the use of facial recognition services, (Effective on July 1, 2021), https://app.leg.wa.gov/billsummary?BillNumber=6280&Initiative=false&Year=2019.

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

[90] [90] U.S. *House Oversight and Reform Committee: Facial Recognition Technology: Ensuring Transparency in Government Use, part II,* (June 4, 2019) (statement of Kimberly J. Del Greco Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation), https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Wstate-DelGrecoK-20190604.pdf.

- FBI policy strictly governs the circumstances in which facial recognition tools may be used, including what probe images may be used.
- The FBI uses FRT 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.
- Trained examiners at the FBI review and evaluate every query is reviewed and evaluated 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 evaluate algorithm performance.[91]

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

### 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 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."[92]

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 at the incident. The ability to efficiently generate investigative leads allows law enforcement to leverage their limited resources. In addition, the use of FRT can confirm any eye-witness identification of the perpetrator, which increases the credibility of such testimony and raises the confidence level of any resulting conviction.

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

The use of FRT by law enforcement and the commercial sector is growing exponentially due to its potential, for law enforcement and other purposes. At the same time, there are significant concerns about potential misuse of such technology by government agencies. 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.

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.[93] Agencies should focus on how to comply with constitutional principles, applicable statutes, and local laws. In addition, the policies should promote transparency regarding the use of FRT.

### 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.

[91] Del Greco, *Facial Recognition Technology, Part II*.
[92] 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.
[93] Law Enforcement Imaging Technology Task Force (LEITTF), *Guiding Principles for Law Enforcement's Use of Facial Recognition Technology,* (Alexandria, VA: International Association of Chiefs of Police, October 17, 2019), 1, https://www.theiacp.org/resources/document/guiding-principles-for-law-enforcements-use-of-facial-recognition-technology.

# Deliberative and Pre-decisional

Many jurisdictions that have adopted restrictions on use of FRT have done so without evidence of documented misuse of the technology by law enforcement. As such, the regulations are often unnecessarily restrictive and based on potential issues.

As more policymakers and the public consider regulations governing the use of FRT, law enforcement agencies should engage with policymakers to provide relevant information that balances competing interests. Law enforcement agencies should collect and share concrete examples of instances where the use of FRT successfully helped investigate or prevent criminal activity. Any adopted internal policies and guidelines on the use of FRT should also be made available to the public. Law enforcement should actively educate the public on steps taken to deter misuse, the amount of training required for its use, and the adoption of transparency measures, which should in turn help make the public confident that law enforcement uses FRT in a responsible and reasonable manner.