ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms

ASHLEY JOHNSON, ERIC EGAN, AND JUAN LONDOÑO I JANUARY 2023

Police tech could transform the way law enforcement operates, reducing crime and saving lives. Policymakers should focus on advancing adoption while enacting regulations to maximize the benefits and minimize the risks of police tech.

KEY TAKEAWAYS

- Artificial intelligence (AI) and machine learning, robotics, biometrics, sensors, cameras, and other technologies can help police prevent, respond to, and solve crime, as well as improve officer safety, training, and accountability.
- Opponents of police tech cite a number of arguments, often with the goal of banning it altogether. There are some legitimate concerns behind the police's use of technology, but bans are not the answer.
- More research and independent testing of police tech, as well as rules governing cybersecurity, transparency, training, and data collection, would minimize many of its risks.
- One of the main obstacles to police tech adoption is budget constraints. The federal government should play a role in advancing adoption via funding to federal law enforcement and grants to police departments.

CONTENTS

INTRODUCTION

Emerging technologies such as AI, robotics, drones, augmented and virtual reality (AR/VR), and the Internet of Things are transforming and improving many sectors. Therefore, it should come as no surprise that these technologies are poised to do the same for policing. Since at least the 1920s, the United States has seen law enforcement adopt new technologies, such as fingerprinting, two-way radios, and databases, to improve their productivity and effectiveness.[1] But technological adoption has often been slow. The President's Crime Commission in 1967 noted, "The police, with crime laboratories and radio networks, made early use of technology, but more policy departments could have been equipped 30 or 40 years ago as well as they are today."[2] Today a suite of existing and upcoming technologies can allow law enforcement to do their jobs more safely, efficiently, and effectively. Widespread adoption of these technologies at all levels of law enforcement would result in more crimes solved (and possibly prevented), more lives saved, greater safety for officers, and taxpayer dollars put to better use.

However, there are many obstacles to greater adoption of technology by law enforcement. In response to a series of highly publicized instances of police killings of Black Americans—including George Floyd, Philando Castile, and Breonna Taylor—a nationwide movement to increase police oversight and accountability has gained steam.[3] Some in this movement have issued calls to defund or even abolish police forces.[4] Others have called for targeted reforms such as restrictions on use of force, creating a duty to intervene in instances of police misconduct, improving misconduct reporting, and ending qualified immunity to reduce police violence and reduce structural discrimination against people of color within the U.S. criminal justice system.[5]

Some digital rights and civil libertarian organizations, which have a long history of opposing police's use of technology, have tapped into this new wave of public anger with law enforcement to launch new campaigns against law enforcement's use of technology, or "police tech."[6] Common criticisms highlight the potential for surveillance, misuse or abuse, and racial or other bias. They also point out the cybersecurity concerns, lack of transparency, and a need to evaluate police tech's effectiveness. While some of these concerns are legitimate, some are born more out of "worst-case scenario" arguments and slippery-slope fallacies and are a smokescreen for police tech bans. This is why many police tech critics conflate legitimate concerns with worst-cases speculation and offer little in the way of solutions to address these concerns other than banning law enforcement from using certain technologies that have the potential to cause harm.

But banning this promising set of technologies would cut law enforcement and the general public off from the many substantial benefits of police tech. Moreover, it would eliminate opportunities to use technology to address police violence, bias, and accountability civil rights groups have been working toward. Rather, the Department of Justice (DOJ), state lawmakers, and police departments should accelerate the testing and deployment of police tech while at the same time creating rules, regulations, and best practices for police tech that would protect the public, curtail misuse and abuse, eliminate bias, and ensure transparency and effectiveness.

This report first explains the different types of police technologies and how law enforcement currently uses them or may use them in the future. Then it outlines and responds to the common criticisms of police tech. Finally, it recommends solutions for advancing adoption and addressing the legitimate criticisms of police tech to maximize benefits and minimize risk, including:

- DOJ should conduct independent testing of police tech that may display bias to guide police procurement.
- DOJ should tie federal funding for police tech to baseline minimum cybersecurity requirements.
- DOJ should establish a police tech grant challenge.
- DOJ's Bureau of Justice Statistics (BJS) should conduct more research on the effectiveness police tech.
- Congress should increase technology budgets for federal law enforcement agencies.
- State lawmakers should regulate police data collection.
- State lawmakers should pass transparency requirements for police departments.
- More police departments should establish voluntary programs that allow residents to share doorbell camera footage.
- Police departments should require officers to complete training programs before using new police tech.
- Police departments should require officers to only use police tech as intended by its developers.
- Police departments should mandate basic cyber hygiene training for all officers.
- Police departments should conduct pilot studies on new police tech to ensure its effectiveness in the field.

THE OPPORTUNITIES

There are a variety of technologies police departments have used or may use in the future for every aspect of their jobs that are not limited to preventing, responding to, and solving crime. There are also technological applications for keeping officers safe, streamlining back and front office processes, improving officer training, and maintaining public oversight and accountability.

These applications rely on AI and machine learning, robotics, biometrics, sensors, cameras, and other technologies, often in combination. Law enforcement and police tech entrepreneurs are only just beginning to tap into the potential of these technologies, such as AI algorithms that can predict where crime is likely to occur, robots that can wade into hostage situations without risking human life, facial recognition algorithms that can help find missing children and identify known criminals, gunshot detection that can drastically reduce the time it takes police to respond to an incident, and body-worn cameras that can help ensure police accountability.

Some technologies, such as DNA identification and traffic enforcement cameras, have been in use for decades, with established rules and best practices for their use. Others, such as predictive policing algorithms and facial recognition, are more recent and potentially controversial additions to the law enforcement tool kit. Law enforcement, government, civil rights advocates, and other stakeholders are still working out the rules and best practices for these emerging technologies.

Preventing Crime

Effective law enforcement helps reduce crime rates. As such, technologies designed to help law enforcement prevent crime rely on AI and machine learning to predict when and where crimes are likely to occur. These technologies build on old techniques law enforcement used before the development and deployment of AI.

Law enforcement has used crime mapping, a technique that aims to predict where crime is likely to occur based on where it has occurred in the past, for hundreds of years to study the relationship between crime and various geographic or demographic characteristics and to help police departments decide where to concentrate their resources. Early crime mapping involved physical maps officers marked with pins to represent recent crimes. With the advent of computers, police could do the same using a virtual map, and in the 1990s began using a tool specifically developed for crime mapping known as a geographic information system (GIS).[7]

A GIS is more interactive than earlier crime maps. When officers add a pin to a physical map to represent where a crime took place, the only information that pin displays is the location of the crime. When officers add a point to a digital map, they can also add information about the exact time and date the crime took place along with other details of the crime that may be useful for analysis.[8]

A GIS also contains data layers officers can use to organize data, with each layer containing a different type of data. For example, one layer may display the roads that run through an area, and a layer on top of that may display the bus routes that run on those roads, and a layer on top of that may display the bus stops along those routes. These layers could be viewed independently or together, stacked on top of each other.[9]

With all the data contained in a GIS, police departments can analyze trends in criminal activity, but the software only contains historical data and cannot make predictions. In the past decade, advances in technology have allowed law enforcement to more accurately predict crime, a technique known as "crime forecasting," which builds on crime mapping.[10]

Crime forecasting, or predictive policing algorithms, uses historical crime and demographic data and data collected by police patrols and stakeouts, from social media, and by other police technologies such as drones, facial recognition cameras, license plate recognition, and body cameras. The algorithms then identify patterns in criminal activity and predict crime with greater accuracy than human analysis can.[11] These predictions give law enforcement the opportunity to deploy their resources more effectively.[12]

Several studies have evaluated the accuracy and effectiveness of machine learning algorithms at forecasting crime. A review of the available literature conducted in 2019 by researchers from Utrecht University finds mixed results, with some studies showing that predictive algorithms are effective and some showing no statistically significant results. Positive outcomes are mostly associated with algorithms that predict where crime is likely to occur, as opposed to who was likely to commit crime.[13] Predictive policing can thus be useful for helping police departments determine where to allocate resources, such as more officers or street cameras.

Due to concerns surrounding efficacy, public opinion, and budget, some early adopters of predictive policing have since shelved their programs, including the Los Angeles Police

Department (LAPD) and Chicago Police Department. The New York Police Department (NYPD) has been using its own in-house predictive policing software since 2013.[14]

Responding to Crime

Law enforcement also has technologies, including gunshot detection, drones, and thermal imaging, to more quickly, safely, and effectively respond to crime.

Gunshot detection relies on sensors equipped with microphones placed around an area. The sensors constantly record audio and monitor for the sound of gunshots. When at least three sensors detect a possible gunshot, they transmit the audio to humans who review the audio and alert the local police.[15]

ShotSpotter, a popular vendor for gunshot detection, provides its services to more than 120 cities and claims a 97 percent accuracy rate.[16] The company places between 15 and 20 sensors per square mile, at least 20 feet above the ground to minimize ambient noise.[17] The goal is to reduce the amount of time it takes to dispatch officers to the scene of a shooting and hopefully, in the long term, reduce gun violence.[18]

In California, ShotSpotter alerted the Oakland Police Department (OPD) to more than 6,000 gunshots in 2020, 91 percent of which were not called in to the police, meaning the OPD may not have been able to respond, especially not in a timely manner. These numbers include 22 homicides and 101 shooting victims. The OPD was able to provide emergency medical response to the 101 surviving victims quicker than if ShotSpotter hadn't alerted the police to the incidents. In some cases, police and medical response took less than two minutes.[19]

A GIS can also be used for similar purposes, with the goal to increase officer productivity, particularly the amount of time it takes them to respond to a crime in progress. The Lincoln Police Department (LPD) in Nebraska tested a GIS app that identifies the locations of persons of interest—including parolees, sex offenders, gang members, and others—in real time. All 75 police officers who tested the app reported that they would recommend the app to others, and a cost-benefit analysis suggests that the app could save the LPD around $800 per officer every five years due to increased productivity.[20]

Police can also use unmanned aerial vehicles (UAVs), colloquially known as "drones," to respond to crime. In many instances, drones can save law enforcement time and money when responding to crime; they are faster than sending officers on the ground and significantly cheaper than helicopters. They are typically equipped with cameras that can capture images and record or livestream video, and may also be equipped with other technologies such as thermal imaging.[21]

The most common law enforcement's use of drones, according to a 2020 survey by the Police Executive Research Forum (PERF), is for search and rescue operations, such as searching for missing persons.[22] Drones can cover a lot of ground and livestream footage back to central command, allowing police to conduct searches remotely.

In the wake of Hurricane Ian in September 2022, several drone teams, featuring members from local sheriff's offices and fire departments and the Florida Department of Law Enforcement, assisted in search and rescue operations. The teams flew drones over areas impacted by the hurricane to provide on-the-ground search and rescue teams with information that helped them allocate resources and coordinate their efforts more effectively.[23]

Another common application area is crime scene photography and reconstruction, including traffic collision reconstruction.[24] Drones take photos of all angles of a crime scene or collision, which officers can later use when they attempt to reconstruct what occurred at the scene.

Drones may be equipped with thermal imaging capabilities, or police may use thermal imagers on the ground. Thermal imagers convert infrared radiation—part of the electromagnetic spectrum that is invisible to the human eye and shows the heat that objects or living things emit—into a visible format. Thermal imagers can "see" past smoke, dust, and chemical agents—situations when normal visibility would be reduced.[25]

The Weber County Sherriff's Office Search and Rescue Team in Utah uses drones with thermal imaging capabilities for their missions. In one instance, a drone found a stranded snowboarder and shined a spotlight on him to direct the team to his location. This also helped the snowboarder, who knew even before the team arrived that help was on their way. Once rescuers found the snowboarder, the drone showed them the safest path off the mountain. Because of the drone, the rescue took half the time it otherwise would have.[26]

Law enforcement uses thermal imaging to search for fugitives or missing persons by seeing their body heat. Additionally, objects will sometimes retain a trace of a suspect's body heat, aiding officers in evidence retrieval.[27] According to a 2001 Supreme Court ruling, law enforcement needs to obtain search warrants to use thermal imaging to search a suspect's home in the same way they would need to obtain a search warrant to conduct a traditional search.[28] But they rightly do not need permission to use thermal Imaging In public locations.

Solving Crime

There are a variety of technologies law enforcement can use, has used, or may be able to use in the near future to solve crime. These include cameras, biometrics, location-based services, and photo editing software.

Law enforcement can use cameras and photographs to solve crime, either by capturing an image or video of someone committing a crime, a suspect or victim, or evidence that leads the police to a suspect or victim. Often the cameras that capture this footage are paired with technology that allows for greater analysis.

Law enforcement has used traffic enforcement cameras to enforce traffic laws for decades. Arizona was the first state to begin using speed cameras in 1987, and New York was the first to employ red-light cameras in 1992. Speed cameras use detectors built into either the cameras themselves or the road to measure a vehicle's speed and issue a citation to the owner or driver if their speed exceeds the posted limit by a predetermined amount. Red-light cameras take a photo before a vehicle enters an intersection and while the vehicle is in the intersection and issues a citation if the traffic light was red in both photos.

Some states have laws prohibiting the use of traffic enforcement cameras, while others have rules for their use.[29] Existing evidence suggests that traffic enforcement cameras can be effective at reducing collisions and related casualties if implemented correctly.[30] However, some drivers object to being caught by an automated system as opposed to a human officer—or to being caught in general—and opponents have raised concerns about municipalities using traffic enforcement cameras as a source of revenue, possibly unfairly.[31] These concerns have led to bans in some jurisdictions.

Some modern traffic cameras can automatically capture all the license plate numbers that come into their view. These systems use what is known as automatic license plate recognition (ALPR). In addition to capturing images of license plate numbers, these systems also typically record the precise date, time, and location the image was captured.[32]

ALPR does not capture images of drivers or passengers, only license plates. The International Association of Chiefs of Police (IACP) has issued guidance to police departments on responsible use of ALPR, including maintaining audit logs for every an time officer accesses ALPR data and their justification for doing so in order to prevent misuse or abuse. According to IACP, ALPR data should only be accessed to locate stolen vehicles, suspects, witnesses or victims of violent crimes, or missing persons; to protect critical infrastructure; and for situational awareness during special events.[33]

These days, an increasing number of homes have doorbell cameras equipped with motion detectors that automatically record video of anyone who approaches. Typically, these cameras allow residents to see who is at their door or capture evidence of package theft. But in addition, doorbell cameras sometimes capture footage law enforcement can use to solve other crimes. In the vast majority of cases, residents voluntarily decide whether to share the footage with police, although occasionally law enforcement may obtain the video directly from the technology company via a subpoena or emergency order.[34]

Some police departments offer doorbell cameras to local residents for free or a reduced price in exchange for permission to view the cameras' footage, while others set up networks with current camera owners the police can call or email to request access to their footage in the event of a crime in the area.[35] In Rutherford County, Tennessee, as of 2019, the Sherriff's Office had used security footage from doorbell cameras in two homicide cases and several property crime cases thanks to homeowners agreeing to share their cameras' footage with the police.[36] As of 2021, nearly 1 in 10 U.S. police departments had partnered with Ring, a doorbell and security camera company owned by Amazon, to request video footage from customers (who can opt out of the program if they so choose).[37]

This practice of residents sharing doorbell camera footage builds on existing law enforcement practices using footage from publicly owned cameras or requesting footage from private establishments to solve crime. Retail stores have been using closed-circuit television (CCTV) systems since the 1970s for theft prevention, and the United Kingdom pioneered the use of public CCTV systems for crime prevention in the 1990s—a strategy some American cities later adopted.[38] Multiple police departments have voluntary sharing programs for privately owned security cameras, similar to programs for doorbell cameras, and some even offer incentives to private businesses in high-crime areas to install them.[39]

In addition to cameras, law enforcement often uses biometrics to solve crime. A biometric is a unique physical or behavioral characteristic, something that no two people share. When law enforcement can obtain biometrics (e.g., DNA or fingerprint evidence from a crime scene), it can use these characteristics to narrow down a pool of suspects or, when a suspect has already been identified, as evidence that the suspect committed a crime.[40]

Law enforcement's use of biometrics to solve crime dates back to the early 20th century. The first criminal trial in the United States that used fingerprints as evidence concluded in 1911, and police still use many of the same techniques to evaluate fingerprints as they did then.[41] Fingerprints are highly unique; not even identical twins share the same fingerprints. There are some limitations when police use latent prints, which are fingerprints left behind on surfaces at the scene of a crime. Latent prints can result in false positives or false negatives, but can still be a useful tool for narrowing a list of suspects or building a case against a suspect.[42]

Many decades later, police added another powerful tool to their crime-solving tool kit: DNA evidence. The first conviction based on DNA evidence in the United States occurred in 1987.[43] As with fingerprints, there are limitations to DNA evidence. A full DNA profile will only match with one person, but police can often only obtain partial DNA profiles, which could match with several people. A partial DNA profile can rule out suspects but not definitively confirm the identity of a perpetrator. Additionally, police finding an individual's DNA at the scene of a crime does not always mean that person committed the crime, which law enforcement and the courts often have to take into account.[44]

Police have also begun using a technique known as "genetic genealogy" to identify criminals. In cases where police cannot match a DNA profile found at the scene of a crime to an individual in any police DNA database, they can request genetic data from companies that offer at-home DNA testing to consumers.[45] These at-home tests provide consumers with information about their ethnic background, ancestry, and predisposition to certain diseases.[46] If police can find a relative of the perpetrator in one of these companies' databases, they can use this information to help identify a suspect. Notably, police used this technique in 2018 to identify the Golden State Killer, a serial murderer who operated in California in the 1970s. The suspect they identified, Joseph DeAngelo, ultimately pleaded guilty in 2020.[47]

More recently, law enforcement has been using another biometric tool: facial recognition. Facial recognition compares images of faces in order to estimate their similarities and verify or determine a person's identity.[48] The technology has many law enforcement applications, such as locating missing children, detecting fraudulent activity, solving cold cases, and identifying criminals.[49]

For example, the International Center for Missing and Exploited Children (ICMEC) developed its Global Missing Children Network Engine (GMNgine) that uses facial recognition to search the Internet and dark web for photos matching missing children.[50] Of course, the effectiveness of this technology is directly related to the number of cameras in place and the ability to use facial recognition on the images to identify the children.

Additionally, the New York State Department of Motor Vehicles (DMV) uses its Facial Recognition Technology Program to identify people with more than one driver's license, including those who've stolen another's identity and tried to obtain a driver's license in that other person's name. As of 2017, the program had led to the arrest of 4,000 people.[51]

In 2014, the Federal Bureau of Investigation (FBI) used facial recognition to find a fugitive who'd been on the run for 14 years after facing charges of child sex abuse. A special agent ran FBI wanted posters through facial recognition software that contained images of U.S. visa and passport photos and found a match, leading to the fugitive's arrest in Nepal.[52]

There are many other biometrics, including voice recognition, iris recognition, retina scans, gait analysis, and signature recognition.[53] As technologies continue to develop, law enforcement could use a wide variety of biometrics to solve crimes that, in the past, may have been unsolvable.

There are multiple federal fingerprint and DNA databases law enforcement can access to compare fingerprints or DNA found at a crime scene to those of convicted offenders, arrestees, or detainees. The FBI oversees the Combined DNA Index System (CODIS), a collection of DNA databases that includes the National DNA System (NDIS), deployed in 1998, which contains DNA profiles submitted by federal, state, and local forensic laboratories.[54]

States have differing laws on the collection of arrestee DNA. Some states do not allow police to collect DNA from people who have been arrested but not convicted of a crime. Others allow the practice but have certain restrictions, such as excluding juvenile arrestees or requiring police to expunge the records either automatically or upon request. Most states that allow the collection of arrestee DNA only allow it for felony arrests (not misdemeanors), and several states further restrict the collection to certain felonies.[55] Restrictions on the collection of arrestee DNA protect the privacy of individuals who may have been wrongfully arrested or arrested without enough evidence for a conviction.

The FBI also maintains the Integrated Automated Fingerprint Identification System (IAFIS), deployed in 1999, which contains digital fingerprint data from criminals, detainees, persons of national security interest, federal applicants and employees, immigrants, and the military. In 2011, the FBA deployed its Next Generation Identification (NGI) system to expand on the IAFIS with improved and bolstered capabilities, including a facial recognition search, palm prints, and an iris image repository.[56]

Another controversial technique law enforcement frequently employs to solve crime is location-based services. Geofencing technology uses GPS, RFID, Wi-Fi, and cellular data to set up a virtual boundary within the physical world, called a "geofence."[57] A geofence warrant enables police to ask a tech company for an anonymous list of all the active devices within a geofenced area both during a certain time when and where a crime took place. Police narrow down the list to devices they believe could be connected to the crime and ask the tech company for those users' personal data.[58]

Geofence warrants are a controversial approach, though one law enforcement frequently uses. Google had a 1,500 percent increase in geofence warrant requests from 2017 to 2018 and a 500 percent increase from 2018 to 2019. Concerned over the number of overly broad requests it received—such as warrants requesting data that would identify all users within a certain geographical area and time frame—Google began objecting to any warrant that did not first request de-identified data and then narrow down that data to likely suspects before requesting the users' identities.[59]

Finally, law enforcement can sometimes use photo editing software to solve cases. The National Center for Missing and Exploited Children (NCMEC) has partnered with Adobe since 2007 and uses its software for tasks such as aging up photos of missing children to show what they might look like in the present, helping find over 3,000 children between 2014 and 2018. NCMEC has also used Adobe software to create facial reconstructions of deceased children from scans of their skulls, helping identify over 150 deceased children as of 2020. Finally, NCMEC has used photo editing software to enhance images in order to search for evidence that may lead to the child's location or identify a suspect behind the abuse.[60]

Keeping Officers Safe

Existing and emerging technologies designed to keep officers safe rely on robotics and unmanned or autonomous capabilities. Drones and robots add a layer of separation between human police officers and potential danger, such as a bomb or an armed criminal.

Just as it can use drones to help solve crime, law enforcement can also use drones to help keep officers safe. According to PERF, "investigating armed and dangerous suspects" is the third most common law enforcement use case for drones, tied with disaster response.[61] As an example, during an active shooter incident, drones can livestream aerial footage to law enforcement so officers have intel on the shooter's precise location and the locations of possible casualties.

Active shooter incidents are a real risk to officer safety. From January to September 2022, the FBI reported that 49 law enforcement officers were intentionally killed. Firearms were used in over 80 percent of those deaths. Fifteen of the officers were confirmed to have been wearing body armor when they were killed.[62]

Similarly, law enforcement can use robots to reduce the risk posed to human officers. Law enforcement and the military have used remote-controlled "robots" for bomb disposal for over 40 years. These robots examine and disable unexploded bombs, landmines, and munitions up close while their human operators remain at a safe distance.[63]

Perhaps the most famous modern example of a law enforcement robot is Boston Dynamics' "Spot," a robot dog used in manufacturing and construction as well as by police. The company describes Spot as an "agile mobile robot," with four legs and the ability to navigate spaces and climb stairs.[64] The NYPD acquired its own Spot, dubbed "Digidog," in 2020, but terminated its lease of the robot in 2021 after it became the target of opposition from activists during the "defund the police" movement who claimed Digidog was a representation of overfunded police departments and over-policing in minority communities.[65]

In that time, the NYPD used Digidog six times, including during multiple hostage situations.[66] In February 2021, Digidog was sent into a building in the Bronx to investigate a hostage situation. In October 2020, it was sent into a basement in Brooklyn where witnesses of a shooting said the gunman was hiding. It also delivered food to hostages in a home invasion in Queens.[67]

Back Office/Front Office

At the end of the day, law enforcement agencies are customer service organizations, with many of the same challenges as other government agencies. Through this lens, too, technology provides law enforcement with opportunities to both improve the customer experience and citizen engagement (front office), as well as streamline case management and internal operations (back office).

Case management software—broadly defined as the digital tools that allow an organization to manage its cases—can be transformative for certain administrative-intensive activities in law enforcement, such as chain of custody, which refers to the chronological "paper trail" involving the collection and tracking of evidence.[68] As it includes both electronic and physical evidence, chain of custody is vital in the criminal justice system. Case management software easily accommodates inventory management and digital filing, reducing human error across the various documentation handoffs to ensure evidence is appropriately tracked and chain of custody is maintained.

Modern case management software is frequently cloud-based, offering improved security for sensitive data and greater flexibility for staff and officers to access the software across multiple platforms (e.g., desktop, laptop, mobile, etc.).[69] This is particularly helpful for organizations with field staff, but also improves resilience during emergency situations that disrupt normal operations, as was the case with the COVID-19 pandemic.

Additionally, most case management systems come “out of the box” with data analytics and visualization features that offer organizations insight into their caseload and workflow performance, as well as reporting functions for police departments to easily compile and share statistics or compliance requirements to other local, state, and federal agencies.

Some law enforcement agencies, such as the NYPD, have already rolled out or plan to roll out modern case management systems, but many others continue to rely on manual paper processes or outdated legacy software that is error-prone and inefficient.[70]

On the customer side, mobile technology offers citizens a different access point for police services—one many people are familiar with in their day-to-day lives.[71] A mobile app could allow citizens to easily report a crime on their own behalf or on behalf of others, including level of severity, type of crime, location, and other pertinent details.

Many law enforcement agencies receive an overwhelming number of calls from citizens, most of which are noncriminal or nonurgent.[72] Mobile app messaging services—and even chatbots—offer customers a familiar, accessible method to interact with law enforcement, while also helping to reduce the substantial workload of police dispatch and telecommunicators.

Furthermore, case management software can be integrated with data feeds from citizen-facing mobile apps (as well as existing telephony infrastructure). The case management system generates tasks and initiates workflows based on the citizen request or crime reported, allowing law enforcement officers and staff to prioritize and organize caseloads more efficiently and quickly.

Lastly, the integration of front-office mobile apps and back-office case management technology contributes to fuller communication and improved relationships between citizens and law enforcement agencies. Citizens experience increased transparency through real-time case status and documentation updates fed from the case management software. Likewise, mobile app push notifications allow law enforcement agencies to disseminate critical information to particular areas or communities, such as all-points bulletins and “be on the lookouts” that would be worth sharing with the public about fugitives, missing persons, active shooters, or terrorists—similar to how police issue Amber alerts for missing or abducted children.

Improving Officer Training

Police departments across the country have implemented VR tools to optimize officer training.[73] Police departments have continuously struggled with undertraining, particularly with nonlethal equipment such as tasers. For example, according to a 2010 study funded by the National

Institute of Justice (NIJ), police officers receive an average of eight hours of taser training, with fewer than a quarter of law enforcement agencies exceeding the minimum training standards required or recommended by manufacturers.[74] This lack of training is largely the result of financial, logistical, and knowledge issues, as police departments often do not see training as a priority in terms of funding, which means it is often underfunded.[75] Additionally, training usually requires access to an appropriate venue to conduct these simulations and the presence of a knowledgeable trainer on-site. While a large, urban police department may accommodate these conditions, smaller departments in rural areas often struggle to do so.

The use of VR in officer training allows for a portable, more cost-effective option for police departments, as training can be done anywhere using a VR headset, requiring only the presence of a trained evaluator. Current training offerings allow officers to train with on-demand content online and even use exact, weight-accurate replicas of the actual tools. The immersive content and accurate replicas allow officers to train their muscle memory to make last-second decisions in a high-stress environment in the real world. These online, portable, and on-demand tools allow officers to schedule training in downtime without the need for any special room accommodations and without having to wait for an equipment specialist to be present. This makes it cheaper, more accessible, and more effective than in-person training.

VR training has also shown tremendous promise in empathy and perspective-based training.[76] This type of training could help aid police departments' training in various fields, such as interactions with hard-of-hearing individuals, mental health crisis responses, and racial-sensitivity training. Immersive learning has resulted in a higher empathic response in trainees, allowing them to simulate scenarios that depict the difficulties these communities endure.[77] In these simulations, police officers go through the experience of interacting with the police from the civilian's perspective. For example, in the case of hard-of-hearing simulations, the audio in the simulation is muffled to accurately reflect the difficulties these individuals experience during these scenarios. In cases of domestic violence training, the officer embodies a domestic violence victim trying to interact with the police while in a state of shock, reflected by visual and auditive cues such as a ringing sound.

Exposing police officers to the difficulties these individuals face in their day to day believably and realistically using immersive technology allows officers to understand the particular challenges and experiences these individuals face. Having a better understanding of these challenges might provide police officers with better tools to respond to situations involving members of these communities.

Maintaining Public Oversight and Accountability

There are a number of technologies used to increase police accountability, including cameras worn on police uniforms. These body-worn cameras document officers' actions and serve additional purposes on top of increasing accountability, such as documenting crimes, arrests, accidents, and other incidents and providing video evidence for investigation and prosecution.[78]

The NYPD has the largest body-worn camera program in the United States, with 24,000 officers equipped with these cameras in a three-phased rollout that started in 2017 and concluded in 2019. The purpose of the cameras is to provide an "objective record" of police encounters, and officers are required to record certain events, such as arrests, uses of force, and searches. The NYPD retains video recordings for 18 months.[79]

BJS published a report in 2018 on law enforcement's use of body-worn cameras in the United States. The report finds that by 2016, 47 percent of law enforcement agencies had acquired body-worn cameras; that number increased to 80 percent for large law enforcement agencies. BJS's cost-benefit analysis of body-worn cameras indicates that their benefits to society outweigh the financial costs associated with their use.[80] According to NIJ's CrimeSolutions program, which rates criminal justice practices to evaluate what works, out of seven body-worn camera programs, five had statistically significant benefits, though none had statistically significant benefits in all categories, including use of force, citizen complaints, citizen injury, officer injury, citizen resistance, officer-initiated contact, citations, and arrests.[81]

The evidence on their use for other objectives thus far has shown mixed results. A 2019 meta-analysis of 70 studies of body-worn cameras published by researchers from George Mason University finds that body-worn cameras do not have consistent, statistically significant effects on officer behavior.[82] Some studies show a decrease in uses of force, but other studies show no difference in uses of force between officers wearing cameras and officers not wearing cameras.[83]

Imagining the Future of Police Tech

Even the most well-equipped police departments are only scratching the surface of possibilities when it comes to deploying police tech. As technology continues to improve and costs continue to decline—and especially if the federal government takes the lead in deploying police tech and providing funding for state and local law enforcement—more police departments will take advantage of new and emerging technologies for a variety of applications that will make police more efficient and effective and keep officers and civilians safe.

Preventing Crime

As AI becomes more sophisticated, predictive policing software will become more accurate and therefore even more useful to law enforcement as a crime prevention tool. With AI predicting where different types of crimes are likely to occur, police departments could more efficiently allocate their resources and decrease response times.

Responding to Crime

With improvements in natural language processing, which allows AI to understand and replicate human language, automated dispatchers could answer 911 calls, thereby decreasing the burden on human 911 operators. Gunshot detection and other sensors will alert police to crime as soon as a disturbance takes place, and officers will receive these alerts via apps on their smart devices that will also tell them the location of their colleagues so the officers closest to the scene of the disturbance can respond.

Solving Crime

The more cameras that exist in the world—cell phone cameras, security cameras in or outside homes and private businesses, and city-owned cameras in public spaces—the more likely a crime will be caught on camera. With facial recognition, police will be able to more easily identify suspects, victims, and witnesses from photos or videos, and advanced photo editing and reconstruction capabilities could aid in that process.

Keeping Officers Safe

Police departments will procure robots to take over dangerous tasks and drones to enter dangerous situations ahead of human officers. In an active shooting scenario, police could send a drone to give them an aerial view of the scene before engaging. In a hostage scenario, police could send a robot to provide food and supplies to hostages while hostage negotiators work to resolve the situation. In a scenario wherein police do not know if a suspect is armed and dangerous, they could send in a drone or robot first to assess the level of risk and better prepare officers before they engage.

Back Office/Front Office

In the future, case management will be a fully digital process, streamlining back-office processes so officers spend less time filling out paperwork and more time out in the streets solving crime. Office automation will take even more work off human officers' hands and remove opportunities for human error. Fully digital systems not only save time but also allow for greater cooperation, which is key in law enforcement, as cases sometimes require collaboration between multiple police departments or levels of government.

Improving Officer Training

More officer training will take place in AR and VR environments, allowing officers to train under realistic but safe conditions. Instead of gaining their first experience with dangerous or risky situations on the job, officers could first experience simulations of those situations—such as an active shooter or hostage situation—in a controlled environment. Simulations of police interactions from a civilian perspective could also help officers better understand how to interact with victims, suspects, and witnesses.

Maintaining Public Oversight and Accountability

Cameras will not only be important in identifying persons of interest and creating a trail of evidence, they will also continue to serve as an important tool for public oversight. Officers required to use body-worn cameras will have an additional incentive to follow proper protocol, and evidence from body-worn cameras can hold officers accountable if they break the rules or use unnecessary force. Audit trails in digital systems will help hold officers accountable for how they use new technologies.

THE CRITICISMS

Each of the technologies law enforcement can use has potential benefits for keeping the public safe and bringing criminals to justice. However, many also have potential drawbacks, especially if deployed without appropriate limits and rules. These potential drawbacks have given rise to attacks on the technology from privacy and civil justice advocates and other stakeholders over the potential for police surveillance, as well as legitimate concerns over misuse or abuse of police tech, bias, lack of transparency, cybersecurity, and overall effectiveness.

Some of these concerns are based on real-life examples of misconduct or harm. Others are based more on "slippery slope" arguments and anti-technology sentiment, ignoring the myriad benefits of police technology, if utilized correctly.

Every technology has pros and cons, and when it comes to police technology, the key for maximizing the pros and minimizing the cons will be finding ways to address the top concerns associated with the technologies at law enforcement's disposal through rules and best practices for their procurement and use.

It is important to note that many civil liberties groups that prioritize individual rights over public safety oppose such increases in police technology. Others believe that the U.S. criminal justice system is an inherently racist system, and any increase in police capabilities will lead to the further oppression of racial minorities. Therefore, it is futile to attempt to find a compromise with groups that fundamentally oppose any increase in the technological capabilities of law enforcement.

Surveillance Concerns

One of the most common arguments against police's use of technology is a concern that the use of new and emerging technologies amounts to a form of surveillance.[84] Critics express concern over the erosion of privacy post-9/11 and draw connections to both China's use of mass surveillance to control its population and science fiction dystopias such as the one depicted in *Minority Report*.[85] These critics postulate a world in which Americans would have no privacy in public or potentially even private spaces and law enforcement agencies would track their movements and activities and trample on their constitutional rights.

Surveillance concerns are at the heart of opponents' arguments against ALPR, gunshot detection, facial recognition, geofencing, and drones. These opponents point out that police could use facial recognition and ALPR to track individuals' movements.[86] Because gunshot detection sensors are constantly recording audio, critics are concerned that police could use the sensors for general audio surveillance.[87] Finally, overly broad geofence warrants could mean that "anyone whose commute takes them by the scene of a crime might suddenly become vulnerable to suspicion, surveillance, and harassment by police," according to the Electronic Frontier Foundation (EFF).[88]

There are legitimate concerns attached to law enforcement's use of technologies such as facial recognition, including concerns over how and how long police retain facial recognition data. But these concerns can be addressed through policy, such as setting data retention policies for biometric data. And there are also many benefits attached to these technologies. Surveys show that the majority of Americans support beneficial uses of facial recognition, including by law enforcement.[89]

Banning law enforcement's use of new technologies is not the answer, and lawmakers should not fall for the opposition's arguments. If lawmakers can instead create rules that would limit the risks involved, law enforcement could still get the benefits of these technologies without violating valued civil liberties.[90]

In the case of geofencing, future court cases will likely determine whether law enforcement's current broad use of geofence search warrants is permissible under the Fourth Amendment and potentially establish more concrete guidelines.[91] Notably, in 2022, a U.S. District Judge in Richmond, Virginia, denied a geofence warrant and raised concerns over its constitutionality with police having first established probable cause (as law enforcement must do for all other types of warrants).[92] State and local governments may regulate the use of certain other technologies, as a number of cities have done by banning facial recognition.[93]

Singling out specific risks attached to technologies is legitimate—and there should be rules in place to mitigate those risks. But arguments that rely on hypothetical risks, especially sensational claims that law enforcement's use of certain technologies will "end privacy," leading to bans that will cut law enforcement and the public off from the benefits of technology.[94] In fact, that is the reason certain privacy groups make these claims.

These types of extreme claims are far too common. According to Privacy International, "[T]he radical introduction of [facial recognition technology] will inevitably result in the normalization of surveillance across all societal levels."[95] The American Civil Liberties Union (ACLU) claims, "Automatic license plate readers have the potential to create permanent records of virtually everywhere any of us has driven."[96] Finally, the Electronic Privacy Information Center has argued, "Surveillance from the skies threatens to end privacy in public."[97] It would be more beneficial for civil liberties and public safety if these groups focused their efforts on helping craft appropriate rules that allow widespread use of police technologies with appropriate safeguards.

In addition to fears of broad, widespread surveillance, critics also express concern over the potential for more-targeted surveillance, such as surveillance of protestors, journalists, minority communities, or critics of the police or the government. There are many examples of these types of abuses in nondemocratic countries.[98] However, the United States has strong political rights and civil liberties, guaranteeing Americans free press and the freedom to protest and criticize the government that stand in the way of the United States becoming like China. To the extent law enforcement engages in activities that violate Americans' rights, the practice should be subject to legislative oversight and judicial review so that these practices do not continue.

Ultimately, the fear that police tech will lead the United States down the path toward dystopia is a slippery-slope argument based more on worst-case scenarios than facts. If critics believe that the only thing standing between democracy in the United States and a totalitarian surveillance state is technology, that indicates a problem with society, not with technology. The U.S. court system should and will continue to uphold Americans' constitutional rights regardless of the technology law enforcement uses.

Misuse and Abuse of Tech

A related concern is individual law enforcement officers or entire police departments might misuse or abuse the technology at their disposal, either intentionally (e.g., an officer using police tech to stalk a domestic partner) or unintentionally (e.g., an agency failing to provide its officers with proper training, resulting in misuse). But this is true for any technology, including guns, vehicles, and cameras.

Unlike many surveillance concerns, concerns over potential misuse or abuse of police tech are not merely hypothetical. There is a history of individual police officers violating policy or even the law, and sometimes using police resources to do so. The Associated Press found that officers from state law enforcement agencies and major police departments were fired, suspended, or resigned at least 325 times between 2013 and 2015 for misusing confidential databases. An additional 250 instances of abuse resulted in reprimands, counseling, or other discipline.[99]

Motivated by personal reasons and acting outside their police duties, officers can dig up information on a variety of individuals, such as current or former romantic partners, romantic interests, or journalists who publish negative stories about the officers or their departments.[100] For example, in Massachusetts, an officer who worked for the Lanesborough Police Department was fired in 2021 for using a police database to stalk and harass women.[101]

In the same way officers sometimes misuse or abuse police databases, they could also misuse or abuse other police technology, some of which may collect potentially sensitive personal information about individuals.

Officers may also unintentionally misuse technology if they have not received adequate training on how to use police tech. For example, Washington County police ran police sketches, rather than photos, through Amazon's facial recognition software Rekognition, which is not an appropriate use of the technology and would certainly increase error rates and false positives. Washington County's use of police sketches was only an experiment, but actual use of facial recognition in this way has resulted in false arrests, though it has also resulted in legitimate arrests.[102]

This is not the only example of police misusing facial recognition. A report published by Georgetown Law's Center on Privacy and Technology in 2019 finds that at least half a dozen police departments in the United States permitted officers to run facial recognition searches on police sketches. It also shows examples of police using celebrity look-alikes to run facial recognition searches and editing photos of suspects in ways that could change the results of a facial recognition search, such as replacing an open mouth with a closed mouth or closed eyes with open eyes.[103]

These and other examples of misuse or abuse of police tech and police databases demonstrate that the concern over potential misuse and abuse is legitimate. The potential for misuse or abuse necessitates oversight, over both individual officers' actions and police departments as a whole to ensure that officers receive adequate training and are not using police tech for their own personal benefit outside the line of duty.

Bias

Another popular argument against police tech is a concern that either the technology itself or law enforcements' use of it will result in increased bias, potentially exacerbating existing problems of racial profiling and over-policing of minority communities. Critics frequently cite this argument when it comes to technologies powered by AI or machine learning, claiming that the algorithms that power certain law enforcement technologies are likely to be biased against certain racial, ethnic, or other minority groups.[104]

Ideally, an AI system would be 100 percent accurate and provide purely objective results. But humans create and test AI systems, and thus there is always the possibility of human error and human bias. A significant potential source of bias in an AI system is the data it is trained on. Biased data has a much higher risk of producing biased results. Another potential source of bias comes when humans interpret—or potentially misinterpret—an algorithm's outputs.[105]

In 2018, the ACLU used Amazon's facial recognition software, Rekognition—a technology some police departments also use—to compare photos of members of Congress against a database of mugshots. The ACLU claimed Rekognition made 28 false matches, a disproportionate number of which were for people of color.[106] However, when the ACLU ran this test, it used a confidence threshold of 80 percent. Amazon recommends using a 99 percent threshold.[107] Rather than proving that modern facial recognition technology is inherently biased, the ACLU's test proves that facial recognition technology is more likely to give biased results if used incorrectly.

AI bias isn't only a concern in police tech. Bias in AI systems is a topic of discussion, research, and debate across all AI applications: in healthcare, hiring, housing, education, and more.[108] Notably, the concern about bias in facial recognition has resulted in multiple cities banning government use of facial recognition.[109] Indeed, many of the organizations that criticize law enforcement's use of facial recognition technology, such as the ACLU and EFF, support bans.[110]

In police tech, the concern over AI bias is heightened due to existing racial bias in the U.S. criminal justice system. Studies show that Black people are more likely to be arrested for drug violations than white people despite comparable drug use rates; Black and Hispanic drivers are more likely to have their cars searched; Black drivers are more likely to be arrested during a traffic stop; and Black men are more than twice as likely than white men to be killed by police.[111] And Black and Hispanic people are more likely to receive heavier sentences for similar crimes.[112]

Bias in police tech is a legitimate concern, but not an unsolvable one. Depending on the data an AI or machine learning algorithm is trained on, the quality of the algorithm itself, and the way it's used, AI has the potential to either exacerbate or reduce bias in policing. A report by the National Institute of Standards and Technology (NIST) assessing facial recognition algorithms reveals that the most accurate algorithms display "undetectable" bias and have low rates of false positives and false negatives.[113]

These highly accurate, higher quality algorithms are significantly less biased than humans. It is the less accurate, lower quality algorithms that display significant bias and could lead to biased policing outcomes. Police departments should procure more accurate AI systems and avoid less accurate systems. This would lead to a decrease in biased policing by shifting some of the decision-making from biased humans to unbiased algorithms.[114]

Over-Policing

A related concern to police tech exacerbating bias is police tech exacerbating the problem of over-policing. Over-policing refers to police maintaining an excessive presence, using excessive force, and responding aggressively to minor offenses in certain communities. In the United States, this problem primarily affects poor communities, especially poor communities of color.[115]

For example, critics of gunshot detection argue that the technology may exacerbate over-policing of communities of color. In Chicago, police districts with ShotSpotter had a higher Black and Latino population, whereas districts without ShotSpotter had a relatively higher non-Hispanic white population. As a result, a disproportionate number of Chicago police dispatches related to ShotSpotter were in police districts with a higher Black and Latino population.[116]

Critics of predictive policing make a similar argument. As EFF has pointed out, if police have historically concentrated their efforts on marginalized communities, then the historical data that predictive policing relies on will identify those areas as criminal hotspots and predict that more crime will occur there. Police will respond to the algorithm's predictions by concentrating resources in those communities, which will result in police responding to more crime in those areas, which will perpetuate the cycle.[117]

Police tech can exacerbate over-policing in the same way it can exacerbate bias: through bad data. The predictions of an algorithms are only as good as the data the algorithm has. If a police department has been over-policing communities of color for decades, then the historical data from that police department will be biased toward predicting more crime in those communities. And if cities such as Chicago only use ShotSpotter in police districts with higher Black and Latino populations, then more police will be dispatched to those districts. In other words, over-policing leads to more over-policing.

However, it is also important to consider the need for more police resources in areas with more crime, especially violent crime. In addition to problems of over-policing, many poor communities also face problems of under-policing: lack of adequate police presence or police response to violent crime impacting members of the community.[118] This indicates that a significant part of the problem of over-policing is not simply that there is too large of a police presence in certain communities, but that police focus a disproportionate amount of their energy and resources on responding to minor infractions and perhaps not enough energy and resources on major crime. This is not a problem of police's use of technology, but rather of police training and priorities.

Over-policing is a legitimate concern, but the solution isn't for police to stop using data-driven technologies, but rather take a closer look at how they use data. For example, a police department that has reoriented its strategy away from aggressively pursuing low-level offenses may decide not to use data about certain misdemeanors and instead focus on using data about violent crime.

Lack of Transparency

A concern that touches on every aspect of law enforcement's use of technology is a lack of transparency. Without transparency requirements, individuals would have no way of knowing how police departments are using technology and what they are doing with the data they collect. This makes holding law enforcement accountable for potential abuse or misuse of technology far more difficult, and degrades public trust in law enforcement institutions.

Data-driven technologies, which require police to collect data from the public in order to gain useful insights, are of particular interest to critics of police tech.[119] Examples include facial recognition, predictive policing, gunshot detection, and automated license plate recognition. All these technologies collect some form of data from the public, which may include sensitive personal data (e.g., face scans, in the case of facial recognition, or location data, in the case of ALPR) or more generalized data (e.g., historic crime crates in an area, in the case of predictive policing).

Critics of police tech aren't the only people concerned about a lack of transparency. Transparency concerns have been a major theme in the wider backlash against technology—or "techlash"—that has particularly targeted large tech companies.[120] For example, AI systems, such as those used to moderate content on social media, are often compared to a "black box" because users and researchers have little to no insight into how these algorithms make decisions (although there is also often little insight into how human moderators make decisions).[121] On social media, the worst that can happen to an individual is their account gets banned. But when it comes to law enforcement's use of technology, misuse or abuse could lead to wrongful imprisonment or even death. This makes transparency in law enforcement even more important than in other spheres.

Concerns over a lack of transparency in law enforcement's use of technology are legitimate. Transparency is necessary to ensure adequate public oversight over law enforcement's activities. However, some concerns over police tech have been seemingly counterproductive when it comes to transparency and accountability. For example, digital and civil rights groups have opposed police's use of body-worn cameras out of concern police will use them as a surveillance tool, despite body-worn cameras being an important oversight tool for police behavior.[122]

There are a number of areas where greater transparency is needed. When it comes to body-worn cameras, civilians should know when they're being recorded, and the public should have access to certain body-worn camera footage, such as footage depicting police's use of force. When using technologies that collect data on individuals, departments should share information on what data they collect, why they collect it, how it is stored, and how long it is stored. Departments should also continue to share information on their police tech budgets so taxpayers know where their money is being allocated.

Cybersecurity Concerns

A perpetual concern for any organization's use of technology is bad actors could hack the technology and access, alter, or erase important data. This concern is even more relevant for organizations that collect a lot of sensitive information. For law enforcement, this may include suspects', victims', or witnesses' personal information, evidence against a suspect, or information about an ongoing case.

Cybersecurity should always be top of mind for any organization that uses Internet-connected technology. While robust cybersecurity programs come with costs, these up-front costs are worth it to avoid suffering a significant data breach. According to a 2022 IBM report, the average public sector data breach costs over $2 million.[123] On top of that, organizations often suffer reputational damage after a significant data breach, and individuals whose data has been compromised suffer as well.

In an extreme example of the potential risks of a law enforcement data breach, the Shanghai National Police was the victim of an alleged leak containing police records—including names, addresses, national ID numbers, phone numbers, ages, birthplaces, and incident reports—of one billion Chinese citizens.[124] The data was left unsecured for over a year via a backdoor link that didn't even require a password, and officials didn't become aware of the leak until an anonymous user offered the data for sale in a hacker forum in June 2022.[125] Just two months later, another Chinese government database leaked, this one containing over 800 million records, including photos of faces and license plates.[126]

Closer to home, the Metropolitan Police Department of Washington, D.C., suffered a data breach in 2021, which experts claimed to be the worst known ransomware attack on a U.S. police department. The data breach was the result of a ransomware attack by a Russian-speaking cybercrime syndicate; when D.C. police refused to pay the ransom, the gang released thousands of sensitive documents, including disciplinary files and intelligence reports.[127]

One approach the federal government has taken to cybersecurity, specifically regarding drones, is country-of-origin restrictions. DOJ's Office of Justice Programs (OJP) revised its drone purchasing policy in 2020 to prohibit the use of OJP funds to purchase drones manufactured by certain foreign companies. The Defense and Interior Departments have similar policies that incentivize the procurement and use of U.S.-manufactured drones.[128]

While intended to address the threat of foreign security risks, country-of-origin requirements are a misguided solution. The security of drones—or any other technology—does not depend on where they were manufactured but rather the security controls in place.

Still, cybersecurity is a legitimate concern, as many police technologies collect data that could put officers' or civilians' privacy at risk or even hinder an investigation if it were leaked or tampered with. The location data collected by ALPR and GIS, traditional biometrics such as DNA and fingerprints, suspects' personal phone data obtained via a geofence warrant, body-worn camera footage depicting officers and civilians, and all the other forms of data law enforcement may collect to more effectively keep people safe would be dangerous in the wrong hands.

Effectiveness

The final common argument against law enforcement's use of technology is that, in practice, it may not work as intended and even be less effective than existing methods. Not only would a lack of effectiveness potentially impact law enforcement's ability to solve crimes, it would also be a waste of taxpayer money during a time when many American police departments have already drawn criticism for being overfunded or funds being improperly allocated.[129] This is also often an argument opponents of the technology make as a smokescreen for their real motivation: less-effective policing.

Many police departments have experimented with new and emerging technologies in recent decades and will continue to do so. Sometimes a new technology completely changes the way police do their jobs, as was the case with DNA profiling.[130] Sometimes a new technology has a less revolutionary but nonetheless positive impact, making certain processes safer or more efficient or otherwise aiding officers in doing their jobs. Finally, sometimes police departments adopt a certain technology or implement new technology in a certain way that either fails to improve on existing methods or does not yield enough of a benefit to justify the cost of the technology.

To some extent, this is an unavoidable part of the process of experimenting with new technology. Police departments need to experiment with new technology in order to discover what is effective and determine how to use it in the most effective way. But the concern that certain technologies may be ineffective or a waste of taxpayer money is still a legitimate one, and there have been numerous examples of police departments discontinuing their use of certain technologies when they don't prove effective.

Both the LAPD and the Chicago Police Department ended predictive policing programs due to concerns regarding their effectiveness.[131] In 2019, the LAPD's inspector general released an independent audit on two of the LAPD's predictive policing programs, LASER and PredPol, as well as a third "data-driven policing" program, ELUCD.[132] LAPD deployed LASER in 2011 to identify crime hotspots and reduce violent crime, and deployed PredPol the same year to identify when and where vehicle-related crimes were likely to occur.[133]

While the inspector general's audit did not prove that either of the LAPD's predictive policing programs were ineffective at reducing crime, it also didn't prove that they were effective, and the LAPD discontinued LASER to reassess the program's data.[134] It later discontinued PredPol in 2020 due to budget constraints from the COVID-19 pandemic, although some departments had already stopped using the technology before that due to concerns over its effectiveness.[135]

Meanwhile, the Chicago Police Department discontinued its program, the Crime and Victimization Risk Model (previously known as the Strategic Subject List) in 2020 after the RAND Corporation released a report finding that the program was ineffective at reducing homicides.[136] The program was established in 2012 and aimed to create a list of people most likely to commit or be victimized by a shooting.[137]

It is important to note that the LAPD and Chicago Police Department ending their predictive policing programs also came in the midst of fierce opposition to predictive policing by activist groups, which likely factored into both departments' decisions to stop using predictive policing.

Police departments may choose to discontinue police tech programs for a number of reasons. Budgets, priorities, and public opinion may change and influence what technology a given department uses. One police department may use a certain technology with great success while another department may be dissatisfied with its results from using that technology. Alternatively, a police department may discontinue its use of a certain technology over effectiveness concerns only to later discover how to get the most out of that technology and begin using it again.

For this reason, police departments need to be able to maintain some flexibility over the technologies they use and how they use them. Bans and other overly restrictive regulations fail to provide that flexibility. Rules that govern the use of technology, on the other hand, allow police departments to decide which technologies suit their needs and fit their budgets, while also safeguarding against known risks. Experimentation is a crucial part of the process of adopting new technology. Police tech will continue to improve in its capabilities over time, and police departments' use of police tech will become more effective as they experiment and learn what strategies work better than others.

ADVANCING ADOPTION

The debate surrounding police tech should not only focus on reducing the risks, but also maximizing the benefits. More widespread use of police tech would lead to improvements in policing across the country: more crimes prevented and solved, more officers' and civilians' lives saved, faster response times, more effective training, greater accountability, and more efficient allocation of resources.

Opposition campaigns from advocacy groups are one barrier to police tech adoption. Another is the costs associated with procuring and maintaining various technologies. Robots are a prime example of this. The Digital Vanguard, a bomb disposal robot, costs $31,000.[138] Boston Dynamics' Spot costs $74,500, with optional add-ons such as LIDAR, a camera, an infrared camera, and an arm.[139] These numbers don't include the costs associated with maintaining and operating robots and training officers to use them. For police departments that can afford these costs, robots can pay for themselves in lives saved, but some departments simply do not have the resources to procure and maintain robots.

Drones can also cost a significant amount, though this varies depending on the number and model of drones a police department procures. A basic law enforcement drone costs approximately $800, whereas the most advanced models can run up to $85,000.[140] A program in Scottsdale, Arizona, consisting of two drones and accounting for all the associated equipment and training costs was estimated to cost between $35,000 and $55,000 to establish. This does not account for the continued costs of maintaining a drone program; the Wilmington Police Department in Delaware established a drone program in 2014 and, as of 2020, had spent $200,000.[141]

These costs pale in comparison with the costs associated with police helicopters, which range from $1 million to $10 million to acquire new, or around $500,000 used.[142] Helicopters also come with a high cost per hour to operate, sometimes exceeding $1,000, not accounting for pilots' salaries.[143] But many police departments do not have drones or helicopters. A 2020 study by Bard College finds that 1,103 state, county, and municipal law enforcement agencies had acquired drones, but only 27 percent of those agencies had acquired more than one drone. The average cost of acquisition was nearly $30,000, and a significant majority of agencies acquired their drones via donation or grants.[144]

Even smaller costs can add up. Law enforcement agencies without body-worn cameras reported that the costs associated with the technology—including hardware acquisition, video storage, and system maintenance—were the primary barrier to adoption.[145] Estimates on the cost per camera per year range from $1,221 to $3,219.[146] A small police department with fewer than 10 officers—which accounts for nearly half of U.S. police departments—could therefore end up spending over $10,000 per year equipping its officers with one body-worn camera each.

There is an important role for the federal government to play in providing funding for law enforcement to procure police tech. With more money from Congress, federal law enforcement agencies could not only increase their capabilities but could also set an example of technology adoption and use for state and local law enforcement agencies. The federal government should be a leader in technology adoption, but unfortunately, it often lags behind due to a lack of funding and prioritization.[147]

In addition to taking the lead, the federal government could also provide funding to state and local law enforcement through grants. The federal government does not need to serve as the sole source of funding, but it should make competitive grants available to different-sized police departments in different communities to trial the technology around the country. Finally, the federal government could help counter false narratives about police tech by funding more research into the benefits of it.

RECOMMENDATIONS

Advocates for banning controversial police technologies focus only on the risks of police tech, but there are steps DOJ, state lawmakers, and police departments themselves can take to maximize the benefits of police tech while minimizing the risks. Blanket bans on technology are not the answer; instead, sensible rules and regulations could address critics' legitimate concerns while enabling law enforcement to experiment with new technologies.

Federal Government

- DOJ should conduct independent testing of police tech that may display bias, as NIST has done for a number of facial recognition algorithms during its Face Recognition Vendor Test.[148] Then DOJ should make recommendations to law enforcement to procure technology that displays no significant bias during testing.
- DOJ should tie federal funding for police technology to cybersecurity requirements. These requirements should not include country-of-origin requirements that encourage or discourage procuring systems based on where they were manufactured. Requirements should instead include guidelines police tech must follow in order for departments to procure that technology with DOJ funds. These guidelines should help departments avoid procuring technology that may be vulnerable to attack, and can draw on existing NIST guidance.[149]
- DOJ should establish a police tech challenge competition, with grants to the winners that would go toward procuring police tech, to enable a few smaller or less-funded police departments to test out, benefit from, and become leaders in the widespread adoption of police tech. These departments could then help train other departments around the nation.
- BJS should conduct more research on the effects of different police technologies on important factors such as reducing crime, increasing productivity, and lowering response times. BJS should also continue conducting cost-benefit analyses of police technologies, especially as police tech becomes more affordable and effective and cost-benefit ratios change.
- Congress should increase technology budgets for federal law enforcement agencies of all types to boost adoption of police tech, enabling federal law enforcement to set an example of adoption and effective use of police tech for state and local law enforcement.

State Governments

- State lawmakers should regulate police data collection, including by limiting the amount of time police departments can retain data, with exceptions for data that is potential evidence of a crime, which police may need to retain for long periods of time. Regulations should also only allow the collection of sensitive data for specific purposes related to solving or responding to crime, while the collection of nonsensitive or anonymous data should have fewer restrictions.

- State lawmakers should pass transparency requirements for police departments that would give individuals insight into how police use the data collected, how long that data is stored, and how it is protected.

Local Police Departments

- More police departments should establish voluntary programs that allow residents to share doorbell camera footage with law enforcement when a crime is committed in their area, including partnering with companies that sell doorbell cameras.
- Police departments should develop training programs officers must complete before using new technologies. They should also implement adequate oversight of officers' use of technologies, such as audit logs of digital tools, that would detect misuse or abuse.
- Additionally, police departments should establish rules that officers can only use technology as intended by its developers, such as using the correct confidence intervals for AI or machine learning systems.
- Police departments should require basic cyber hygiene training for all officers and additional cyber training for officers that directly interface with police technology. They should also require system updates as necessary to ensure systems are secure.
- When procuring new technology, police departments should conduct pilot studies to ensure the technology will work as intended in the field, is cost efficient, and is more effective than current methods. They should also conduct regular audits to ensure their programs continue to be effective and cost efficient.

There are real concerns regarding law enforcement's use of certain technologies, but there are also real benefits. By regulating the procurement and use of police technologies instead of banning them, federal and state governments could empower law enforcement to explore new ways of doing their jobs more effectively while minimizing potential risks.

About the Authors

Ashley Johnson (@ashleyjnsn) is a senior policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation, and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

Eric Egan (@ericjohnegan) is a policy fellow for e-government at ITIF. He researches digital transformation in government and how technology can help the public sector achieve mission objectives in innovative and effective ways.

Juan Londoño (@JuanMLondonoR) is a policy analyst focusing on augmented and virtual reality at the ITIF. Prior to joining ITIF, Juan worked as a tech & innovation policy analyst at the American Action Forum, where his research focused on antitrust, content moderation, AR/VR, and the gaming economy. Juan holds an M.A. in Economics from George Mason University and a B.A. in Government & International Relations from the Universidad Externado de Colombia.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org.

ENDNOTES

1. "The Evolution and Development of Police Technology," A Technical Report prepared for the National Committee on Criminal Justice Technology, National Institute of Justice, July 1, 1998, https://www.ojp.gov/pdffiles1/Digitization/173179NCJRS.pdf.
2. "The Challenge of Crime in a Free Society," A Report by the President's Commission on Law Enforcement and the Administration of Justice, February 1967, https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/ncjrs/42.pdf.
3. Kate Whiting, "Black History Month: Key events in a decade of Black Lives Matter," World Economic Forum, February 16, 2022, https://www.weforum.org/agenda/2022/02/black-history-month-black-lives-matter/.
4. Josiah Bates, "How Are Activists Managing Dissension Within the 'Defund the Police' Movement?" *Time*, February 23, 2021, https://time.com/5936408/defund-the-police-definition-movement/; Sean Illing, "The 'abolish the police' movement, explained by 7 scholars and activists," *Vox*, June 12, 2020, https://www.vox.com/policy-and-politics/2020/6/12/21283813/george-floyd-blm-abolish-the-police-8cantwait-minneapolis.
5. "Police Excessive Force," ACLU, accessed October 19, 2022, https://www.aclu.org/issues/criminal-law-reform/reforming-police/police-excessive-force; "Race & Justice," NAACP, accessed October 19, 2022, https://naacp.org/issues/race-justice.
6. Mukund Rathi, "Pushing Back on Police Surveillance: 2021 Year in Review," EFF, December 24, 2021, https://www.eff.org/deeplinks/2021/12/pushing-back-police-surveillance-2021-year-review.
7. Rachel Boba, "Introductory Guide to Crime Analysis and Mapping" (Office of Community Oriented Policing Services, November 2001), https://cops.usdoj.gov/ric/Publications/cops-w0273-pub.pdf.
8. Ibid.
9. Ibid.
10. Joel Hunt, "From Crime Mapping to Crime Forecasting: The Evolution of Place-Based Policing," National Institute of Justice, July 10, 2019, https://nij.ojp.gov/topics/articles/crime-mapping-crime-forecasting-evolution-place-based-policing.
11. Neil Shah, Nandish Bhagat, and Manan Shah, "Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention," Visual Computing for Industry, Biomedicine, and Art 4, no. 9 (2021), https://vciba.springeropen.com/articles/10.1186/s42492-021-00075-z.
12. Beth Pearsall, "Predictive Policing: The Future of Law Enforcement?" National Institute of Justice, June 22, 2010, https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement.
13. Albert Meijer and Martijn Wessels, "Predictive Policing: Review of Benefits and Drawbacks," International Journal of Public Administration 42, no.12 (2019): 1031-1039, https://www.tandfonline.com/doi/pdf/10.1080/01900692.2019.1575664.
14. Tim Lau, "Predictive Policing Explained," Brennan Center, April 1, 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
15. Jay Stanley, "Shotspotter CEO Answers Questions on Gunshot Detectors in Cities," ACLU, May 5, 2015, https://www.aclu.org/news/privacy-technology/shotspotter-ceo-answers-questions-gunshot.
16. "Gunshot Detection," ShotSpotter, accessed October 19, 2022, https://www.shotspotter.com/law-enforcement/gunshot-detection-technology.
17. Stanley, "Shotspotter CEO Answers Questions."
18. "Gunshot Detection," ShotSpotter.

19. Trevelyon Jonees, “Gunshot Location Detection System (ShotSpotter) – 2020 Annual Report” (memorandum to the City of Oakland Chief of Police, June 7, 2021), https://cao-94612.s3.amazonaws.com/documents/Special-Meeting-Packet.pdf.

20. Tom K. Casady et al., “A Randomized-Trial Evaluation of a Law Enforcement Application for Smartphones and Laptops that Uses GIS and Location-Based Services’ to Pinpoint Persons-of-Interest” (University of Nebraska-Lincoln, January 2015), https://www.ojp.gov/pdffiles1/nij/grants/248593.pdf.

21. “Police Drone Infographic,” Dronefly, accessed October 19, 2022, https://www.dronefly.com/police-drone-infographic.

22. “Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks” (Police Executive Research Forum, 2020), https://www.policeforum.org/assets/Drones.pdf.

23. Tarah Jean, “FSU drone team, FAMU faculty assist with Hurricane Ian search and rescue efforts,” *Tallahassee Democrat*, September 30, 2022, https://www.tallahassee.com/story/news/local/2022/09/30/hurricane-ian-search-and-rescue-efforts-aided-fsu-famu-teams/8125717001/; Rebecca Sage, “FSU drone team finishes urban search and rescue work after Hurricane Ian,” *Florida State University News*, October 11, 2022, https://news.fsu.edu/news/university-news/2022/10/11/fsu-drone-team-finishes-urban-search-and-rescue-work-after-hurricane-ian/.

24. “Drones: A Report” (PERF).

25. “Thermal Imaging,” ScienceDirect, accessed October 19, 2022, https://www.sciencedirect.com/topics/earth-and-planetary-sciences/thermal-imaging.

26. Mike Anderson, “Drones are changing search and rescue operations in Weber County,” *KSL*, March 23, 2022, https://www.ksl.com/article/50373531/drones-are-changing-search-and-rescue-operations-in-weber-county.

27. Brad Harvey, “Thermal imaging applications overview for law enforcement,” *Police1*, July 24, 2007, https://www.police1.com/police-products/police-technology/thermal-imaging/articles/thermal-imaging-applications-overview-for-law-enforcement-ssC7sU4JA9onHojm/.

28. David Ruppe, “Supreme Court Rules on Police Using Infrared,” ABC News, June 11, 2001, https://abcnews.go.com/US/story?id=93127&page=1.

29. Jonathan Bates and Shelly Oren, “Enforcing Traffic Laws with Red-Light and Speed Cameras,” NCSL, July 9, 2020, https://www.ncsl.org/research/transportation/enforcing-traffic-laws-with-red-light-and-speed-cameras.aspx.

30. Paul Pilkington and Sanjay Kinra, “Effectiveness of speed cameras in preventing road traffic collisions and related casualties: systematic review,” *British Medical Journal* 330, no. 7487 (2005): 331–334, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC548724/; Ellen G. Cohn et al., “Red light camera interventions for reducing traffic violations and traffic crashes: A systematic review,” *Campbell Systematic Reviews* (2020), https://onlinelibrary.wiley.com/doi/pdf/10.1002/cl2.1091; Katherine Pérez et al., “Reducing Road Traffic Injuries: Effectiveness of Speed Cameras in an Urban Setting,” *American Journal of Public Health* 97, no. 9 (2007): 1632–1637, https://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.2006.093195.

31. Rich Connell, “L.A. red light cameras clicking for safety or revenue?” *Los Angeles Times*, May 20, 2008, https://www.latimes.com/local/la-me-redlight19-2008may19-story.html.

32. “Automated License Plate Recognition,” IACP, accessed October 19, 2022, https://www.theiacp.org/projects/automated-license-plate-recognition.

33. Ibid.

34. Alfred Ng, "Amazon gave Ring videos to police without owners' permission," *Politico*, July 13, 2022, https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513.

35. "Doorbell Camera Surveillance Networks: Community Collaboration to Solve Crime," *COPS Dispatch* 13, no.5 (May 2020), https://cops.usdoj.gov/html/dispatch/05-2020/doorbell.html.

36. Kelsey Gibbs, "Rutherford County police agencies credit doorbell cameras in helping solve crimes," News Channel 5, November 6, 2019, https://www.newschannel5.com/news/rutherford-county-police-agencies-credit-doorbell-cameras-in-helping-to-solve-crimes.

37. Audrey Conklin, "1 in 10 police departments can now access videos from millions of consumers' Ring security cameras," Fox Business, May 19, 2021, https://www.foxbusiness.com/technology/1-in-10-police-departments-amazon-ring.

38. "The Evolution of Closed-Circuit Television (CCTV) Systems," Vector Security Networks, updated January 20, 2021, https://vectorsecuritynetworks.com/the-evolution-of-closed-circuit-television-cctv-systems/; Eric Piza, Joel M. Caplan, and Leslie W. Kennedy, "CCTV as a Tool for Early Police Intervention: Preliminary Lessons from Nine Case Studies," *Security Journal* 30, no.1 (2016): 247–265, https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1185&context=jj_pubs.

39. Craig Rice and Sidney Katz, "Montgomery Council Enacts Bill to Create Private Security Camera Incentive Program," Montgomery County Council, July 26, 2022, https://www2.montgomerycountymd.gov/mcgportalapps/Press_Detail.aspx?Item_ID=41922; "Private Security Camera Voucher Program," D.C. Office of Victim Services and Justice Grants, accessed November 2, 2022, https://ovsjg.dc.gov/page/private-security-camera-voucher-program; "Security Camera Registration," City of Rockville, accessed November 2, 2022, https://www.rockvillemd.gov/2247/Security-Camera-Registration.

40. "Advancing Justice Through DNA Technology: Using DNA to Solve Crimes," Department of Justice, updated March 7, 2017, https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes.

41. Francine Uenuma, "The First Criminal Trial That Used Fingerprints as Evidence," *Smithsonian Magazine*, December 5, 2018, https://www.smithsonianmag.com/history/first-case-where-fingerprints-were-used-evidence-180970883/.

42. William Thompson et al., "Latent Fingerprint Examination" (American Association for the Advancement of Science, September 2017), https://www.aaas.org/sites/default/files/s3fs-public/reports/Latent%2520Fingerprint%2520Report%2520FINAL%25209_14.pdf.

43. *State v. Andrews*, 533 So.2d 841 (Dist. Ct. App. 1989).

44. Naomi Elster, "How Forensic DNA Evidence Can Lead to Wrongful Convictions," *JSTOR Daily*, December 6, 2017, https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions/.

45. Nsikan Akpan, "Genetic genealogy can help solve cold cases. It can also accuse the wrong person," PBS News Hour, November 7, 2019, https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person.

46. Allison Torres Burtka, "AncestryDNA or 23andMe? How to choose the best DNA kit," *Business Insider*, September 27, 2022, https://www.insider.com/guides/health/ancestrydna-vs-23andme.

47. Laurel Wamsley, "Golden State Killer Suspect Pleads Guilty To More Than A Dozen Murders," NPR, June 29, 2020, https://www.npr.org/2020/06/29/884809588/golden-state-killer-suspect-pleads-guilty-to-more-than-a-dozen-murders.

48. "What Is Facial Recognition?" (ITIF, April 2020), https://www2.itif.org/2020-tech-explainer-facial-recognition.pdf.

49. “Face Facts: Dispelling Common Myths Associated With Facial Recognition” (Security Industry Association, June 2019), https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf.

50. ICMEC, “GMCNgine: Revolutionizing the Search for Missing Children,” +SocialGood, March 23, 2018, https://plussocialgood.medium.com/gmcngine-revolutionizing-the-search-for-missing-children-d01772b32e49.

51. Kenneth Lovett, “Facial recognition technology helped lead to more than 4,000 arrests since 2010, Cuomo says,” *New York Daily News*, August 21, 2017, https://www.nydailynews.com/new-york/facial-recognition-tech-helped-lead-4-000-arrests-2010-article-1.3429863.

52. “Long-Time Fugitive Captured: Juggler Was on the Run for 14 Years,” FBI, August 12, 2014, https://www.fbi.gov/news/stories/long-time-fugitive-neil-stammer-captured/long-time-fugitive-neil-stammer-captured.

53. William Miller, “Different Types of Biometrics,” iBeta, September 9, 2019, https://www.ibeta.com/different-types-of-biometrics/.

54. “Frequently Asked Questions on CODIS and NDIS,” FBI, accessed October 19, 2022, https://www.fbi.gov/resources/dna-fingerprint-act-of-2005-expungement-policy/codis-and-ndis-fact-sheet.

55. Charlotte Spencer, “What Is The Arrestee DNA Collection Law In Your State? Biometrica, May 27, 2021, https://www.biometrica.com/what-is-the-arrestee-dna-collection-law-in-your-state/.

56. “Next Generation Identification (NGI),” FBI, accessed October 19, 2022, https://le.fbi.gov/science-and-lab-resources/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi.

57. Tom Nelson, “Geofencing: What It Is and How It Works,” Lifewire, November 10, 2021, https://www.lifewire.com/what-is-geofencing-41612 74.

58. Dean Mirshahi, “Geofence warrants – how police use your phone’s location data and a recent Virginia court ruling,” WRIC, April 5, 2022, https://www.wric.com/news/virginia-news/geofence-warrants-how-police-use-your-phones-location-data-and-a-recent-virginia-court-ruling/.

59. *United States v. Chatrie*, No. 3:19-cr-130 (E.D. Va. 2022).

60. Rachel Kaser, “How Adobe Photoshop is used in the search for missing children,” *The Next Web*, July 24, 2020, https://thenextweb.com/news/adobe-photoshop-used-search-missing-children.

61. “Drones: A Report” (PERF).

62. “Law Enforcement Officer Deaths 01/01/2022–09/30/2022” (FBI, October 2022), https://s3-us-gov-west-1.amazonaws.com/cg-d4b776d0-d898-4153-90c8-8336f86bdfec/LEOKA_INFO.pdf.

63. Peter Ray Allison, “What does a bomb disposal robot actually do?” BBC, July 15, 2016, https://www.bbc.com/future/article/20160714-what-does-a-bomb-disposal-robot-actually-do.

64. “Spot,” Boston Dynamics, accessed October 19, 2022, https://www.bostondynamics.com/products/spot.

65. Mihir Zaveri, “N.Y.P.D. Robot Dog’s Run Is Cut Short After Fierce Backlash,” *The New York Times*, April 18, 2021, https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html.

66. Ibid.

67. Stacy Liberatore, “Robot dog to the rescue! NYPD unleashes its four-legged ‘Digidog’ in the Bronx that uses its cameras and AI to investigate a hostage situation,” *Daily Mail*, February 23, 2021, https://www.dailymail.co.uk/sciencetech/article-9292077/NYPD-unleashes-four-legged-robo-dog-Digidog-Bronx-investigate-hostage-situation.html; Zaveri, “N.Y.P.D. Robot Dog.”

68. “Chain of custody,” NIST Computer Security Resource Center, accessed October 19, 2022, https://csrc.nist.gov/glossary/term/chain_of_custody.

69. Michael Vizard, “AWS Adds More Tools to Secure Cloud Workloads,” Security Boulevard, July 26, 2022, https://securityboulevard.com/2022/07/aws-adds-more-tools-to-secure-cloud-workloads/.

70. Thomas Brading, “OSI modernizing case management platform,” Office of Special Investigations, February 25, 2022, https://www.osi.af.mil/News/Article-Display/Article/2947008/osi-modernizing-case-management-platform/; “Governor Hochul Announces $50 Million in Public Safety Funding at 2022 Division of Criminal Justice Services Symposium,” Governor Kathy Hochul, September 28, 2022, https://www.governor.ny.gov/news/governor-hochul-announces-50-million-public-safety-funding-2022-division-criminal-justice; Mark Geremia, “Paperwork Burden in Policing,” *Police Chief Magazine*, June 19, 2019, https://www.policechiefmagazine.org/paperwork-burden-in-policing/.

71. “Mobile Fact sheet,” Pew Research Center, updated April 7, 2021, https://www.pewresearch.org/internet/fact-sheet/mobile/.

72. Joel Rubin and Ben Poston, “LAPD responds to a million 911 calls a year, but relatively few for violent crimes,” *Los Angeles Times*, July 5, 2020, https://www.latimes.com/california/story/2020-07-05/lapd-911-calls-reimagining-police; Jeff Asher and Ben Horwitz, “How Do the Police Actually Spend Their Time?” *The New York Times*, June 19, 2020, https://www.nytimes.com/2020/06/19/upshot/unrest-police-time-violent-crime.html.

73. Juan Londoño, “How Extended Reality Tools Can Improve Training for First Responders,” (ITIF, June 17, 2022), https://itif.org/publications/2022/06/17/extended-reality-tools-can-improve-training-for-first-responders/.

74. Michael R. Smith et al., “A Multi-Method Evaluation of Police Use of Force Outcomes: Final Report to the National Institute of Justice” (Police Executive Research Forum, July 2010), https://www.ojp.gov/pdffiles1/nij/grants/231176.pdf.

75. Scott Harris, “Product Feature: Less-Lethal Weapons Require Training to Be Effective Force Options,” *Police Chief Magazine*, September 14, 2018, https://www.policechiefmagazine.org/prod-feature-less-lethal-weapons/.

76. Ellysse Dick, “The Promise of Immersive Learning: Augmented and Virtual Reality’s Potential in Education” (ITIF, August 2021), https://www2.itif.org/2021-ar-vr-education.pdf.

77. Insook Han, Hyoung Seok Shin, Yujung Ko, Won Sug Shin, “Immersive virtual reality for increasing presence and empathy,” *Journal of Computer Assisted Learning* 38, no.4 (April 2022): 1115–1126, https://onlinelibrary.wiley.com/doi/10.1111/jcal.12669?af=R.

78. “Body-Worn Cameras” (International Association of Chiefs of Police, April 2019), https://www.theiacp.org/sites/default/files/2020-06/BWCs%20June%202020.pdf.

79. “Body-Worn Cameras,” NYPD, accessed October 19, 2022, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page.

80. Ibid.

81. “Research on Body-Worn Cameras and Law Enforcement,” National Institute of Justice, updated January 7, 2022, https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement.

82. Cynthia Lum et al., “Research on body-worn cameras: What we know, what we need to know,” Criminology & Public Policy 18 (2019): 93-118, https://cebcp.org/wp-content/uploads/2020/06/BWCpaperLumetal.pdf.

83. Ibid.

84. “Street-Level Surveillance,” EFF, accessed October 20, 2022, https://www.eff.org/issues/street-level-surveillance.

85. “Surveillance Under the USA/PATRIOT Act,” ACLU, accessed October 20, 2022, https://www.aclu.org/other/surveillance-under-usapatriot-act; Simon McCormack, “When Minority Report Becomes New Yorkers’ Reality,” ACLU, October 11, 2016,

https://www.aclu.org/news/national-security/when-minority-report-becomes-new-yorkers-reality; David Carroll, "China embraces its surveillance state. The US pretends it doesn't have one," *Quartz*, July 23, 2019, https://qz.com/1670686/the-us-has-a-lot-in-common-with-chinas-surveillance-state/.

86. "You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements" (ACLU, July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf; Adam Schwartz, "Resisting the Menace of Facial Recognition," EFF, October 26, 2021, https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition.

87. "Acoustic Gunshot Detection," EFF, accessed October 20, 2022, https://www.eff.org/pages/gunshot-detection.

88. Matthew Guariglia, "Geofence Warrants and Reverse Keyword Warrants are So Invasive, Even Big Tech Wants to Ban Them," EFF, May 13, 2022, https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants.

89. Ashley Johnson, "New Polls Show Facial Recognition Supported By Majority of Americans, Raising More Doubts About the Merits of Bans," (ITIF, November 30, 2021), https://itif.org/publications/2021/11/30/new-polls-show-facial-recognition-supported-majority-americans-raising-more/.

90. Daniel Castro, "Testimony of Daniel Castro Before the House Committee on Oversight and Government Reform" (ITIF, January 15, 2020), https://www.congress.gov/116/meeting/house/110380/witnesses/HHRG-116-GO00-Wstate-CastroD-20200115.pdf.

91. *United States v. Chatrie*.

92. Ibid.

93. Ashley Johnson, "Banning facial recognition technology: Baltimore's bad idea," *The Baltimore Sun*, June 2, 2021, https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0603-facial-recognition-technology-ban-20210602-edoub7ntkrbxdluonlsrqobgaa-story.html.

94. "Drones and Aerial Surveillance," EPIC, accessed October 20, 2022, https://epic.org/issues/surveillance-oversight/aerial-surveillance/.

95. "Facial Recognition," Privacy International, accessed October 20, 2022, https://privacyinternational.org/learn/facial-recognition.

96. "You Are Being Tracked" (ACLU).

97. "Drones and Aerial Surveillance," EPIC.

98. James Clayton, "China surveillance of journalists to use 'traffic-light' system," BBC, November 29, 2021, https://www.bbc.com/news/technology-59441379.

99. Sadie Gurman, "AP: Across US, police officers abuse confidential databases," *AP News*, September 28, 2016, https://apnews.com/article/699236946e3140659fff8a2362e16f43.

100. Ibid.

101. Thomas Kika, "Officer Fired for Allegedly Using Police Database to Stalk, Harass Women," *Newsweek*, August 3, 2021, https://www.newsweek.com/officer-fired-allegedly-using-police-database-stalk-harass-women-1615920.

102. Isobel Asher Hamilton, "A US police force is running suspect sketches through Amazon's facial recognition tech and it could lead to wrongful arrests," *Business Insider*, May 2, 2019, https://www.businessinsider.com/us-police-running-sketches-through-amazon-facial-recognition-tech-2019-5.

103. Clare Garvie, "Garbage In, Garbage Out," *Georgetown Law Center on Privacy & Technology*, May 16, 2019, https://www.flawedfacedata.com/.

104. Vincent Southerland, “With AI and Criminal Justice, the Devil is in the Data,” ACLU, April 9, 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-and-criminal-justice-devil-data.

105. Bill Siwicki, “How AI bias happens – and how to eliminate it,” *Healthcare IT News*, November 30, 2021, https://www.healthcareitnews.com/news/how-ai-bias-happens-and-how-eliminate-it.

106. Natasha Singer, “Amazon’s Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says,” *The New York Times*, July 26, 2018, https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

107. Daniel Castro and Michel McLaughlin, “Banning Police Use of Facial Recognition Would Undercut Public Safety,” (ITIF, July 30, 2018), https://itif.org/publications/2018/07/30/banning-police-use-facial-recognition-would-undercut-public-safety/.

108. Leo Anthony Celi et al., “Sources of bias in artificial intelligence that perpetuate healthcare disparities—A global review,” PLOS Digital Health 1, no. 3 (2022), https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000022; Miranda Bogen, “All the Ways Hiring Algorithms Can Introduce Bias,” *Harvard Business Review*, May 6, 2019, https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias; Andre M. Perry and Nicol Turner Lee, “AI is coming to schools, and if we’re not careful, so will its biases,” Brookings, September 26, 2019, https://www.brookings.edu/blog/the-avenue/2019/09/26/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases/; Charlton McIlwain, “AI has exacerbated racial bias in housing. Could it help eliminated it instead?” *MIT Technology Review*, October 20, 2020, https://www.technologyreview.com/2020/10/20/1009452/ai-has-exacerbated-racial-bias-in-housing-could-it-help-eliminate-it-instead/.

109. Johnson, “Banning facial recognition technology.”

110. Kate Ruane, “Biden Must Halt Face Recognition Technology to Advance Racial Equity,” ACLU, February 17, 2021, https://www.aclu.org/news/privacy-technology/biden-must-halt-face-recognition-technology-to-advance-racial-equity; Nathan Sheard and Adam Schwartz, “The Movement to Ban Government Use of Face Recognition,” EFF, May 5, 2022, https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition.

111. “Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System” (The Sentencing Project, April 19, 2018), https://www.sentencingproject.org/publications/un-report-on-racial-disparities/; Justin Nix et al., “A Bird’s Eye View of Civilians Killed by Police in 2015,” Criminology & Public Policy 16, no. 1 (2017): 309-340, https://onlinelibrary.wiley.com/doi/epdf/10.1111/1745-9133.12269.

112. “Report to the United Nations” (The Sentencing Project).

113. Michael McLaughlin and Daniel Castro, “The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist” (ITIF, January 2020), https://www2.itif.org/2020-best-facial-recognition.pdf.

114. David Moschella, “AI Bias is Correctable. Human Bias? Not So Much” (ITIF, April 2022), https://www2.itif.org/2022-defending-digital-05.pdf.

115. “Report to the United Nations” (The Sentencing Project); Delores Jones-Brown and Jason M. Williams, “Over-policing Black bodies: the need for multidimensional and transformative reforms,” *Journal of Ethnicity in Criminal Justice* 19, no.3-4 (2021): 181–187, https://www.tandfonline.com/doi/full/10.1080/15377938.2021.1992326.

116. “ShotSpotter is deployed overwhelmingly in Black and Latinx neighborhoods in Chicago,” MacArthur Justice Center, accessed October 20, 2022, https://endpolicesurveillance.com/burden-on-communities-of-color/.

117. Matthew Guariglia, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing," EFF, September 3, 2020, https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing.

118. Rod K. Brunson, "Protests focus on over-policing. But under-policing is also deadly," *The Washington Post*, June 12, 2020, https://www.washingtonpost.com/outlook/underpolicing-cities-violent-crime/2020/06/12/b5d1fd26-ac0c-11ea-9063-e69bd6520940_story.html.

119. NACDL's Task Force on Predictive Policing, "Recommendations on Data-Driven Policing," National Association of Criminal Defense Lawyers, October 24, 2020, https://www.nacdl.org/Content/Recommendations-on-Data-Driven-Policing.

120. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 2019), https://www2.itif.org/2019-policymakers-guide-techlash.pdf.

121. Justin Stoner, "Inside the Black Box: Facebook, Content Moderation, and Machine Learning," *Medium*, November 6, 2020, https://jstoner-614.medium.com/inside-the-black-box-facebook-content-moderation-and-machine-learning-68e7b0e726b1.

122. Matthew Guariglia and Adam Schwartz, "The Justice in Policing Act Does Not Do Enough to Rein in Body-Worn Cameras," EFF, March 2, 2021, https://www.eff.org/deeplinks/2021/03/justice-policing-act-does-not-do-enough-reign-body-worn-cameras.

123. Jonathan Reed, "The Cost of a Data Breach for Government Agencies," *Security Intelligence*, September 7, 2022, https://securityintelligence.com/articles/cost-data-breach-government-agencies/.

124. Karen Hao and Rachel Liang, "China Police Database Was Left Open Online for Over a Year, Enabling Leak," *The Wall Street Journal*, July 6, 2022, https://www.wsj.com/articles/china-police-database-was-left-open-online-for-over-a-year-enabling-leak-11657119903?mod=djemalertNEWS.

125. Yong Xiong, Hannah Ritchie, and Nectar Gan, "Nearly one billion people in China had their personal data leaked, and it's been online for more than a year," CNN, July 5, 2022, https://www.cnn.com/2022/07/05/china/china-billion-people-data-leak-intl-hnk/index.html.

126. Zack Whittaker, "A huge Chinese database of faces and vehicle license plates spilled online," *TechCrunch*, August 30, 2022, https://techcrunch.com/2022/08/30/china-database-face-recognition/.

127. Alan Suderman, "DC Police victim of massive data leak by ransomware gang," *AP News*, May 13, 2021, https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9.

128. Daniel Castro and Ashley Johnson, "Drone 'localization' policies will backfire," *The Hill*, December 8, 2020, https://thehill.com/opinion/cybersecurity/529190-drone-localization-policies-will-backfire/.

129. Rashawn Ray, "What does 'defund the police' mean and does it have merit?" Brookings, June 19, 2020, https://www.brookings.edu/blog/fixgov/2020/06/19/what-does-defund-the-police-mean-and-does-it-have-merit/.

130. Retro Report, "How DNA Changed the World of Forensics," *The New York Times*, May 18, 2014, https://www.nytimes.com/video/us/100000002886783/how-dna-changed-the-world-of-forensics.html.

131. Lau, "Predictive Policing Explained."

132. Mark P. Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies" (Los Angeles Police Commission Office of the Inspector General, March 2019), http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

133. Ibid.

134. Mark Puente, “LAPD ends another data-driven crime program touted to target violent offenders,” *Los Angeles Times*, April 12, 2019, https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html.

135. Caroline Haskins, “The Los Angeles Police Department Says It Is Dumping A Controversial Predictive Policing Tool,” *Buzzfeed News*, April 21, 2020, https://www.buzzfeednews.com/article/carolinehaskins1/los-angeles-police-department-dumping-predpol-predictive; Mark Puente, “LAPD pioneered predicting crime with data. Many police don’t think it works,” *Los Angeles Times*, July 3, 2019, https://www.latimes.com/local/lanow/la-me-lapd-precision-policing-data-20190703-story.html.

136. Jessica Saunders, Priscillia Hunt, and John S. Hollywood, “Predictions put into practice: a quasi-experimental evaluation of Chicago’s predictive policing pilot,” *Journal of Experimental Criminology* 12 (2016): 347-371, https://link.springer.com/article/10.1007/s11292-016-9272-0.

137. Kathleen Foody, “Chicago police end effort to predict gun offenders, victims,” *AP News*, January 23, 2020, https://apnews.com/article/41f75b783d796b80815609e737211cc6.

138. “Vanguard Robot Assessment” (Office of Justice Programs, July 2022), https://www.ojp.gov/pdffiles1/nij/204637.pdf.

139. Evan Ackerman, “Boston Dynamics’ Spot Robot Dog Now Available for $74,500,” IEEE Spectrum, June 16, 2020, https://spectrum.ieee.org/boston-dynamics-spot-robot-dog-now-available; “Spot,” Boston Dynamics.”

140. “Drones: A Report” (PERF).

141. Ibid.

142. Rick James, “Police Helicopters: All Your Questions Answered,” Pilot Teacher, October 14, 2021, https://pilotteacher.com/police-helicopters-all-your-questions-answered/.

143. Erin Wisti, “What Is Going On With LAPD Helicopter Surveillance?” *Knock LA*, March 21, 2021, https://knock-la.com/lapd-helicopter-surveillance-6ed93fb7c9a/.

144. Dan Gettinger, “Public Safety Drones, 3rd Edition” (Center for the Study of the Drone at Bard College, March 2020), https://dronecenter.bard.edu/files/2020/04/CSD-Public-Safety-Drones-3rd-edition.pdf.

145. Shelley S. Hyland, “Body-Worn Cameras in Law Enforcement Agencies, 2016” (Bureau of Justice Statistics, November 2018), https://bjs.ojp.gov/content/pub/pdf/bwclea16.pdf.

146. Morgan C. Willians, Jr. et al., “Body-Worn Cameras in Policing: Benefits and Costs” (National Bureau of Economic Research, March 2021), https://www.nber.org/system/files/working_papers/w28622/w28622.pdf.

147. Ashley Johnson and Daniel Castro, “Improving Accessibility of Federal Government Websites” (ITIF, June 2021), https://www2.itif.org/2021-improving-accessibility-federal-government-websites.pdf; Ashley Johnson and Daniel Castro, “Assessing the Federal Government’s Transition to Web-Based Forms” (ITIF, August 2021), https://www2.itif.org/2021-federal-government-web-form.pdf.

148. Patrick Grother, Mei Ngan, Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects” (NIST, December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

149. Jon Boyens et al., “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations” (NIST, May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.