Emerging Police Technology: A Policy Toolkit

CRIMINAL JUSTICE POLICY PROGRAM
HARVARD LAW SCHOOL

Stanford Law School
Stanford Criminal Justice Center

Contents

Advisory Board

Matt Cagle, Technology and Civil Liberties Policy Attorney, ACLU of Northern California

Amy Condon, former Chief Legal Advisor, Boston Police Department

Catherine Crump, Assistant Clinical Professor and Director of the Samuelson Law, Technology & Public Policy Clinic, Berkeley School of Law

Ronald Davis, former Director of the Office of Community Oriented Policing Services, U.S. Department of Justice

Alfred Durham, former Police Chief, Richmond (VA) Police Department

Isaiah Fields, General Counsel, Axon

Andrew Ferguson, Professor of Law, University of District Columbia School of Law

Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law

Sharad Goel, Assistant Professor, Department of Management Science & Engineering, Stanford University

Elizabeth Joh, Professor of Law, University of California-Davis

Eric Jones, Chief of Police, Stockton (CA) Police Department

Nicole Jones, Senior Law Enforcement & Security Counsel, Google

Vivek Krishnamurthy, Counsel, Foley Hoag LLP, and Affiliate, Berkman Klein Center for Internet & Society at Harvard University

David Roberts, Executive Director, Search Group, Inc.; former Senior Program Manager, IACP Technology Center

Adam Schwartz, Senior Staff Attorney, Electronic Frontier Foundation

Sameena Usman, Government Relations Coordinator, Council on American-Islamic Relations

Reilly Webb, Executive Director, Texas Governor Greg Abbott's Criminal Justice Division

Acknowledgments

Emerging Police Technology: A Policy Toolkit was prepared by the Criminal Justice Policy Program at Harvard Law School and the Stanford Criminal Justice Center at Stanford Law School. Research and drafting were contributed by Harvard Law School students Rebecca Martin, Michael Roig, Natalie Salmanowitz, Jonathan Eubank, Keerthana Medarametla, Gene Park, Megan Lee, and Timothy Yap; and Stanford Law School students Julie Goldrosen, Robert Paris, Katie Kelsh, Drew Flood, Leah Yaffe, and Michael Poon. The toolkit drafting was overseen by Colin Doyle, Staff Attorney at CJPP; Mason Kortz, Clinical Instructor at the Harvard Law School Cyberlaw Clinic; Elana Fogel, Legal Fellow at CJPP; Brook Hopkins, Executive Director of CJPP, Debbie Mukamal, Executive Director of Stanford Criminal Justice Center; David Sklansky and Robert Weisberg, Faculty Co-Directors of the Stanford Criminal Justice Center; and Carol Steiker and Alex Whiting, Faculty Co-Directors of the Criminal Justice Policy Program.

How To Use This Toolkit

Modern police technologies pose an enormous challenge for police departments. License plate readers, drones, body cameras, and gunshot detection systems, for example, are powerful data-collection, data-creation, and data-retention tools. The value in these technologies is the information they generate. Their challenge is in collecting, managing, and using that information responsibly.

This toolkit begins with an introduction that describes this challenge and explains how smart, forward-thinking approaches are necessary in order to avoid mistakes and mismanagement. Next is a worksheet designed specifically for police chiefs to use as they consider acquiring new technology. The rest of the toolkit is divided into three sections that examine in detail the interconnected issues that data-collection technologies invariably cause police department leaders to face: Costs, Governance, and Community. Each section briefly summarizes challenges, outlines helpful practices for addressing them, and provides worksheets to help manage the process. The Governance and Community sections also include checklists which contain solutions and best practices.

An appendix at the end of the toolkit collects all of the worksheets and checklists in one place.

Introduction

Law enforcement agencies across the country are adopting new technologies at a rapid pace. Automated license plate readers, facial recognition systems, and predictive policing software are now common policing tools for big and small departments alike. Undeniably, modern technology has transformed the nature of police work. Police departments can now uncover, collect, create, and share troves of new information and integrate this data across devices and agencies.

Data-generating police technologies require new rules and new ways of thinking about long-term costs and controls. Acquiring data-collection technology is unlike other equipment procurement because the costs and downstream effects are connected not just to the physical hardware but to the resulting data governance required. Police departments are not just buying investigative tools, they are buying data systems that must be controlled and managed.

The mistakes and errors of past surveillance technology rollouts have resulted from not seeing this important difference between devices and data. Mismanaging technology can result in exorbitant financial costs, leave private data vulnerable to hackers, and damage a department's relationship with the community.

As technology has transformed policing practices, police departments and legislative bodies have struggled to keep pace with the associated issues and challenges. Police departments sometimes procure devices before establishing internal policies. And the cities and states that have begun to regulate police technology often take a piecemeal approach, designing policies for one specific technology at a time. Police departments and state and local regulators lack flexible, forward-thinking guidance that cut across multiple technologies.

The Stanford-Harvard Project on Technology and Policing was created to fill the gaps in police technology policy. PTP is a collaborative effort of Stanford Law School's Criminal Justice Center and Harvard Law School's Criminal Justice Policy Program. By bringing together law enforcement, state and local officials, lawyers, activists, technologists, community groups, and academics, we aim to identify crosscutting policy issues and develop helpful guidance for police departments, government regulators, and advocates.

PTP Roundtable Policy Discussion

In the fall of 2017, PTP held a roundtable policy discussion on policing technology with 24 national experts. Participants included local and state policymakers, law enforcement leaders, activists, academics, a technologist, and industry representatives with diverse backgrounds and a range of perspectives. Participants uniformly agreed that police departments should adopt policies for the procurement and use of new technologies, but also expressed concern that departments often lack the policy guidance they need.

In response to the concerns raised at the roundtable discussion, PTP created this toolkit to help police departments when considering new technology. Most of the roundtable participants are now members of PTP's advisory board and have provided valuable ideas and feedback for the toolkit.

Police Chief Worksheet

Before purchasing any new technology, consider these big picture questions.

1. Why does my department need this technology?

2. What public safety problem(s) does this technology help solve?

3. Is this public safety problem a priority or a distraction from more important issues in our community?

4. What is the full capacity of this technology—in other words, what does it do and what kinds of data does it collect beyond my organization's needs?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

5. Does the purchase of this technology require approval from legislative bodies, boards, or commissions?

6. What control will my department have over the data that is collected? Who will own it?

7. Who will have access to the data?

8. What are the privacy implications of this technology?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

9. What kind of legal liability could this technology bring?

10. How will my department protect data we collect?

11. How might this technology change my department's relationship with the community? How will deploying this technology affect my officers' day-to-day interactions with our community?

12. What concerns might the public have?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

13. How will my department listen to the public about this technology?

14. What independent research has been done to evaluate this technology? (Independent research is not paid for by developers or vendors of the technology or their agents.)

15. How has this technology worked out in other jurisdictions?

16. How much will it cost? Consider: hardware, software, maintenance, data storage, data security, staffing, training, and compliance with open record laws and policies.

The Data Challenge

Police have always adopted new technologies to help keep society safe. Over the years, innovations like police radios, computers in squad cars, and DNA testing have significantly changed and improved law enforcement, allowing police to do their work with more insight, efficiency, and effectiveness. But today's data-collection technologies are so powerful and entail such a problematic set of issues that new approaches to procurement, policies, and planning are imperative.

Today's smart phones and police cars have the ability to collect data about location, time, activity, and behavioral patterns. No longer just ordinary tools, these smart devices now create sophisticated data trails that can be mined for training, accountability, and use in civil or criminal litigation. Police surveillance technologies only add to this complexity. As digital cameras, body cameras, and sensors advance in sophistication, the ability to monitor the community and collect data on people grows in previously unimaginable ways. Police are now in the data business and must plan for this new role.

This toolkit addresses three data challenges: costs, data governance, and community relations. A clear understanding of each issue will help police departments adopt efficient, responsible, and effective policies.

Costs
Modern policing technologies generate substantial financial costs beyond an initial hardware or software purchase. By anticipating these future expenses, police departments can make more informed choices about which technologies are worth adopting.

Governance
Poor data management jeopardizes data privacy, accuracy, and reliability. Police departments can mitigate these risks through sensible data governance policies.

Community
New technologies can strengthen or weaken a department's relationship with the community. Regular public engagement and transparent policies allow police departments to build trust with the communities they serve.

Promising new digital technologies seem to appear every day. All present problems of data collection. If police departments don't have a strategic plan, they can be easily overwhelmed by data. From budgets to security to public trust—so much is at stake.

01 Costs

Data-generating technologies impose different costs than more traditional policing tools. That's because maintaining data has additional costs that can grow exponentially over time—including the costs involved with managing and mitigating risk. This section outlines the costs of acquiring data-generating technologies: Risk, Lifecycle, and Hidden Costs

Risk

Anticipating and managing risk is complex and time-consuming, but learning how to detect, prevent, and recover from mistakes and legal disputes will save considerable time, money, and frustration over the long run.

When a police department collects and retains data, it takes on the responsibility to safeguard it, ensure it is used appropriately, and comply with any applicable laws and regulations. Failure to do so means the department risks being held legally, financially, and publicly accountable—for example, if the data is misused or a data breach occurs.

Taking on these additional risks and responsibilities is costly. Departments should factor in the following costs when considering the adoption of any new data-collection technology:

Litigation
New police technologies are sometimes challenged in court. The cost of defending against a lawsuit can greatly increase the cost of a technology.

Public Record Requests
Emerging technologies generate troves of data—all of which may be subject to a state or local government's public record laws. Compliance with these laws can require dedicated personnel to process requests, comb through databases, and redact complicated files (including video and audio files).

Privacy
Surveillance technologies decrease the privacy of the communities that police serve and often decrease privacy for police officers themselves. This cost is determined by the capabilities of the technology, not the intent of the purchaser.

Community Relations
The public is often skeptical of new technology, especially technology that can infringe on privacy or is deployed only in certain neighborhoods. Overusing or misusing surveillance technology can erode community trust. Police departments around the country have accidentally leaked supposedly secure data, an embarrassing, costly, and potentially dangerous mistake that undermines police-community relations.

Real Risk:
Vendor Error

Costly Data Breaches

In June of 2019, U.S. Customs and Border Protection reported that images collected at the border of people's faces and license plates were stolen in a cyberattack of its subcontractor Perceptics. This private vendor had violated CBP policy by transferring the images to its corporate network. The breach brought increased scrutiny and criticism from lawmakers and privacy advocates at an already tense time of national debate over the use of data-collection technology for law enforcement.

01 Costs

Police departments increasingly use sophisticated technologies to gather important data that helps them more effectively fight crime and protect the public. But ensuring that data is secure and properly processed, analyzed, shared, and finally archived becomes exponentially more challenging—and expensive—over time.

Lifecycle

The data lifecycle is everything that happens to a piece of information from the moment it is collected to the moment it is deleted. This includes migrating data from one system to another when storage technologies are updated.

Maintaining data throughout its lifecycle requires significant resources: storage space, computing power, backups, security, an interface to access and use the data, staff time, and more. Because of this, data-generating technologies have ever-growing costs that continue long after the hardware is acquired. These increased costs come in many forms.

Storage
Some technologies, especially video capture systems like body cameras and ALPRs, generate huge amounts of data. The cost of storing that data can quickly exceed the cost of acquiring the systems themselves. Some companies even offer free hardware because their real profits come from charging for data storage and maintenance.

Migration
When new technology replaces old technology, data must be moved from an old system to a new one. This means either spending staff time on the transition or hiring a vendor or outside consultant. There also can be added costs to make that new technology compatible with existing systems.

Staffing
Although police technologies can improve efficiency, more data often means more work. Officers may spend a significant amount of time each shift inputting, uploading, downloading, processing, browsing, searching, or otherwise handling data. For larger departments, getting the most out of data often means hiring specialized staff, such as a data analyst or long-term consultant.

Court Prep
Even if day-to-day use of the data doesn't require a specialist, use of the data in a trial may. In order to use data from police technologies at trial, departments need to be able to identify Brady material, respond to requests for evidence from the prosecution and defense, and get the data into formats that court systems can use and that judges and jurors can understand.

Legal Compliance
As local and state governments continue to amass more data, state legislatures are passing regulations that mandate how data must be stored, how long it must be retained, and how it must be made available to the public. As these laws proliferate, police departments can encounter unexpected cost increases for technologies that they've already purchased.

Community Oversight
Independent of any legal requirement, police departments often have their own transparency policies for disclosing information to the community. As a police department deploys more technology, it must also invest more time and energy into complying with these policies to maintain community trust.

01 Costs

Understanding the hidden costs of new technologies helps police departments make smart decisions, select the right tools, and reduce unnecessary expenditures.

Hidden Risks

Data-generating technologies often come with unknown capacities and consequences. Hidden risks are often impossible to identify, but there are specific areas where we know these risks can hide.

Vendors
Vendors are understandably eager to tell police about the benefits of their products—especially free ones. But "free" technology is rarely free for long. Vendors often offer free tools so they can charge for services later once a department has become dependent upon the technology.

Academic and Independent Research
Many academic institutions and independent research organizations examine the effectiveness of police technologies. Unfortunately, they do so with varying amounts of rigor, making it difficult to know which ones to trust. Sometimes a flawed research report can undermine the legitimate use of a technology. Good research on the other hand can help predict the effectiveness and impact of a new technology, but results are seldom universally applicable. Conclusions drawn from studying large, urban departments, for example, may not be applicable to smaller, rural departments, and vice versa.

Other Police Departments
With around 18,000 police departments in the United States, the chances are good that other nearby departments will have experience using and maintaining the same technology and are often the best resource for learning about unexpected costs. When considering the drawbacks to a technology, a police department can't limit itself to thinking only of the department's own potential problems. Lawsuits or protests challenging another jurisdiction's use of a police technology can have national consequences affecting the viability of using the technology elsewhere.

Real Risk:
Bodycams

Technology Purchased and Abandoned

Police departments are abandoning once-promising bodycam programs because the costs of maintaining them have spiraled out of control. The East Dundee, Illinois police department ended its bodycam program because the data storage costs grew too big. And police in Wahoo, Nebraska ended their bodycam program because a new state data-retention law sent the cost of maintaining the program through the roof.

The Washington Post quotes Jim Pasco, executive director at the National Fraternal Order of Police: "The easy part is buying the body cameras and issuing them to the officers. They are not that expensive. But storing all the data that they collect–that cost is extraordinary. The smaller the department, the tougher it tends to be for them."

Costs Worksheet

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

1. Are there ongoing costs associated with maintaining the technology or storage equipment? What are the typical costs for a department of our size?

2. Does the vendor provide assistance with transition from older systems? What about transitioning away from the technology if we change vendors in the future?

3. Does the vendor provide training? Does this training fit the needs of our police department?

4. How much does the training cost? How much time does the training take?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

5. Does this technology rely on a proprietary (secret) software that is inaccessible to the police or the public? Are there alternatives available?

6. Has there been any litigation over the use of the technology, either against the company or against a police department that uses the technology?

7. Can our police department control what types of data are collected?

8. Can our police department control who has access to the data collected and can it share it with other entities?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

9. Where is the data we collect stored?

10. Is the vendor prohibited from using, sharing, or selling the data without express permission of our police department?

11. Does the vendor provide security software with this product? Does the software meet the security standards of our state, municipality, and department?

12. Does the vendor use data collected by the police or collect data beyond the needs of law enforcement? If so, how is the company using that data?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

13. Have independent studies been conducted on the effectiveness of the technology? (Independent studies are those not conducted or paid for by developers or vendors of the technology or their agents.)

14. Does our department need to sign a non-disclosure agreement to acquire the technology?

02 Governance

The data challenge makes smart data governance and management indispensable. Data governance is the creation and implementation of a strategy to ensure data best serves the needs of its organization. It determines the policies and practices that consistently keep data safe, accurate, relevant, and reliable. Data management is the administrative process that supports that strategy by appropriately collecting, securing, storing, organizing, sharing, archiving, and deleting data. Data governance and management work hand in hand. This section defines and explains some of their major goals.

Policies for data collection and management ensure that sensitive, useful information remains protected, accessible, and trustworthy.

Security

Sound data governance greatly benefits police departments and the public they serve by providing:

- Better protection of individual privacy
- Lower risk of cyber-attack
- Lower risk of staff misuse or abuse of technologies
- Increased accountability

The right time to create your data governance plan is before you begin collecting data. The decision not to collect data is always the first line of privacy protection. Data that is never collected cannot be lost, leaked, or misused. When a police department decides to collect data, the department should be able to articulate:

- How the data will be used
- What type and what amount of data will be collected
- With whom will the data will be shared
- When the data will be deleted
- Who in the department can read or edit the data

Many technologies collect data that can be used to identify specific individuals. This type of data must be managed carefully so that it is stored securely with strict access controls. Certain types of sensitive data must be handled with particular care under state and federal laws like HIPAA and FERPA which prohibit the disclosure of medical and educational histories.

02 Governance

Training Personnel

Many data breaches are caused by avoidable internal errors rather than by external attacks. Employee training has been proven to significantly reduce such errors, yet many local agencies often have difficulty finding qualified data security personnel, let alone training the rest of their employees.

The Department of Homeland Security and the National Institute of Standards and Technology provide a list of resources that can help departments improve security awareness. Private companies also provide data security training. Even with these resources, training diverts time from other important police activities. Therefore, departments often choose a two-tiered plan for data security training:

Tier One
Employees who work directly with sensitive data and have the capability to add, delete, alter, or share this data receive comprehensive security training before being granted access.

Tier Two
Employees who do not work directly with this data also receive training, but this training focuses on spotting common security risks rather than understanding the inner workings of security frameworks, standards, and technologies.

Training is an essential part of any data governance plan—even the most comprehensive policy is ineffective if users do not follow it.

Limiting Access

An access policy determines who has access to a dataset, network, or device. It also determines how much access each person has. The best access policies require logging all access and activity. Access policies can, if necessary, also restrict which devices a certain dataset is accessible on. For example, mobile phones and devices that can connect to public wifi networks are notoriously unsafe.

The best practice in creating an access policy is the principle of least privilege. This means that each person should only have as much access as they need to do their job. For example, a dataset could allow personnel to search through some data but prevent them from being able to alter or delete any of it. Access isn't an all-or-nothing prospect. Users can always be granted higher privileges temporarily if necessary for certain projects. But having an access policy is critical.

Deleting Data

The longer a police department retains its data, the greater the likelihood its data will be disclosed—deliberately or by accident. Over time, many types of data can become less useful for law enforcement purposes. That same data, however, still contains sensitive information. More data means more potential security breaches.

There are many approaches to setting data retention plans. One option is to use one deletion schedule for all of the department's data. A more nuanced plan may be preferable since the usefulness of certain kinds of data will expire faster than others. Some data types may become irrelevant after 24 hours, while others may remain useful for years. Data should not be stored after its usefulness has expired.

Data deletion can be automated. Automation is often desirable because it can be difficult for personnel to be faithful to data retention schedules; human error and day-to-day business can prolong the storage of data when its deletion is neglected. Departments that do not automatically delete data often set periodic notifications that remind appropriate staff members when to purge data.

02 Governance

Sharing Data

Advances in technology have made data sharing easy and commonplace. Police departments often share data with fusion centers that pool evidence, intelligence, and other data across local jurisdictions and states nationwide.

Data security is only as strong as its weakest link. It doesn't matter how securely a department protects sensitive data if it is shared with an organization that does not have equally strong protections. Not everyone takes good care of their data. Even governmental agencies and other police departments may not apply adequate rigor or care to their data security.

Because increased data sharing results in higher risk of data breach and leaks, police departments must determine whether the entities who can access shared data are secure. Shared access to data requires a policy governing shared data control. Resources like the National Criminal Intelligence Sharing Plan help identify the best policies to implement for your department.

It's not enough for your department to have secure data-sharing practices. The other departments and organizations you share data with must, too.

Police departments also need to be careful about accidentally sharing information with agencies whose practices conflict with a police department's own policies and mission. For example, many police departments and local jurisdictions have policies against cooperation with U.S. Immigrations and Customs Enforcement (ICE). But a recent investigation reveals some of these departments subscribed to a vendor's automatic license plate reader database without knowing that ICE was also subscribed to the database. By contributing information to the database, some of these departments may have unintentionally violated both internal policies against cooperation with ICE and their local sanctuary city laws.

Auditing

Data governance policies often include periodic audits, both to determine policy compliance and to aid in the development of new policies. To enable auditability, every data interaction should be logged, including but not limited to collection, searches, access, and integration. Although data-generating technologies are often less visible than many traditional policing tools, they are also more auditable.

While law enforcement agencies should implement internal auditing procedures, independent third-party audits should also be conducted periodically to ensure objectivity and accuracy. Auditing the use of the voluminous data sets collected by police can be a challenge because of the sheer amount of activity.

Real Risk:
Ransomware

Data Held Hostage

In recent years, hackers have infected police departments around the country with "ransomware" viruses that lock police out of their own systems. Affected departments have to choose between paying off the hackers and losing access to their data–which can mean losing months of work. Ransomware attacks can also cost cities millions of dollars in security fixes.

Governance Worksheet

When a police department collects data, it must be able to articulate every aspect of its data governance and management plans. These questions are some of the most important to answer.

1. What type of data will we collect?

2. Why do we need this data?

3. How will we use this data?

4. Could this data be used in ways that might raise concerns for our community?

Governance Worksheet (Continued)

When a police department collects data, it must be able to articulate every aspect of its data governance and management plans. These questions are some of the most important to answer.

5. Who in our department will be able to access this data and when?

6. Who will we share this data with?

7. When will we delete this data?

Governance Checklist

Use this checklist to make sure you're covering the most important aspects of your data governance and management plans.

1. Dataset integration

Police departments collect many kinds of data. Although individual datasets may be benign, problems may emerge when coupled with other datasets. Consider, for example, that each dataset may contain information about a piece of a person's life. As datasets become linked, they will form a more complete profile of that person. Dataset integration may make for effective policing, but it also raises increased privacy concerns.

- ☐ Avoid data integration if it is not absolutely necessary for legitimate law enforcement purposes.

2. Security Protocol

For a sample security policy, see the FBI's Criminal Justice Information Services ("CJIS") Security Policy. For a general introduction to institutional data security, see the U.S. Department of Homeland Security Computer Emergency Readiness Team ("US-CERT") security publications. More guidelines can be found at the National Institute of Standards and Technology ("NIST") Computer Security Resource Center.

Include these security protocol basics to ensure your data is secure:

- ☐ Strong password protocol and standards for all devices
- ☐ Effective antivirus and malware software and policies
- ☐ Stringent, limited access policies
- ☐ Limited connection to the internet
- ☐ Frequent purges to eliminate former users

3. Training

In order to keep data secure, reduce employee errors, and help keep staff accountable, your department should incorporate the following two tiers of training:

- ☐ Tier One Training: all employees receive training focused on best practices and spotting common security risks
- ☐ Tier Two Training: employees who work directly with sensitive data and have the capability to add, delete, alter, or share this data, receive specialized security training

4. Limited access

- ☐ Make sure only personnel who absolutely need data–especially sensitive data–have access to it.
- ☐ Maintain a comprehensive inventory of personnel who have access to sensitive data.
- ☐ Monitor and audit user access to sensitive data.

Governance Checklist (Continued)

Use this checklist to make sure you're covering the most important aspects of your data governance and management plans.

5. Data Sharing

- ☐ Keep track of who we share data with and why.
- ☐ Frequently review whether those we share data with still need it.
- ☐ Vet the organizations we plan to share data with to make sure they have adequate security policies and practices.

6. Data Retention

- ☐ Decide whether automatic or manual deletion approaches are best for each dataset your department collects.

7. Audits

Third-party audits are necessary to protect police data adequately. Some security loopholes escape even the most competent computer users.

- ☐ Use third party auditors to verify that what appears secure is actually secure.

03 Community

Modern policing depends upon strong community relationships. Technology has the potential to strengthen the relationship between the police and the community. Police can interact with community members on social media, issue electronic alerts and advisories, and provide opportunities for public accountability by soliciting feedback and releasing data and video.

But new policing technology can also undermine a department's relationship with its community by intruding upon privacy interests and targeting specific populations for surveillance. Community engagement is essential. When police acquire and use surveillance technology in secret, refuse to disclose how technology is being used, and resist public record requests, community relations fall apart.

In many cities and towns, police departments more heavily patrol and surveil minority and poor communities that have higher crime rates. Taken together, the many forms of police technology—security cameras, license plate readers, gunshot detection systems, and more—can indiscriminately record the entire public life of a neighborhood. Accordingly, police technology can disproportionately encroach upon the privacy of poor communities and communities of color. In many places, a legacy of government discrimination or a history of police violence means that these same communities do not trust the police to use surveillance technologies in a fair and equitable way. This distrust can be hard for departments to overcome.

Careless deployment of technology can reopen old wounds or create new rifts between police and the public. Technology that was acquired to support investigations can undermine investigations if police cannot also rely on the support and trust of their community. Recognizing this, some departments have opted out of using certain technologies, not because the department feared that its officers would misuse the technology, but because the department acknowledged that any use of the technology would damage the department's relationship with the community.

When community relationships are not managed properly, police technology can invite public skepticism, distrust, and protest.

Real Risk:
Public Backlash

Grounded Drones

In 2010, the Seattle Police Department used over $80,000 in federal funds to purchase surveillance drones. But the department never informed Seattle's City Council—the local body in charge of the department's budget—about this purchase. In fact, the Council did not learn about the department's drones until two years later, when the Federal Aviation Administration released a report that listed the Seattle Police Department as an authorized drone user. This revelation invited backlash from the public and the City Council. In response to the bad press and public protests, the police department shut down its drone surveillance program without ever using the equipment.

03 Community

Community Meetings

A police department should hold community meetings prior to technology procurement and deployment to keep the public informed and get feedback. Soliciting public input informs the community, informs the police, and builds legitimacy for police using a technology in the future. Early community feedback and involvement helps the community to be a partner in policing efforts and prevents the public from feeling blindsided by new or expanded uses of policing technologies. By listening to community voices early in the procurement process, police departments can also ensure that public funds are not spent on technology that the community will reject.

Community meetings serve two important goals. First, they allow police to educate the community and correct misconceptions about technology and how police plan to deploy it. Second, they allow the communities most likely to be affected by these technologies to educate the police about their concerns. Without these meetings, communities and police risk talking past each other and holding mistaken assumptions about the other's objectives, actions, and motives.

Better policies come from cooperation and dialogue. Community meetings are an opportunity for the police to inform the public and for the public to inform the police.

Dialogue helps clear up misconceptions. In many instances, the public may be concerned about the nefarious deployment of surveillance technology that police have not even contemplated. For example, a police department may acquire surveillance technology thinking that it would be useful for emergency situations like terrorist attacks. The public fears that the police will use the technology to conduct regular surveillance in certain residential neighborhoods that are already heavily policed. Through community engagement, police departments can clear up misconceptions and the public can share their concerns. In response to community concerns raised at these meetings, police can enact policies limiting how a new technology is used.

Operating Policies

An operating policy describes how a department will–and won't–use a given technology. It prevents confusion and miscommunication about appropriate use of a new technology. Without an operating policy, a police department cannot set a standard for responsible use of the technology and will be unable to identify misconduct. Without defining guidelines or limits, police departments won't be able to assure the public with credibility that the technology will be used only in a responsible way.

Operating policies can be shared publicly on a department's website with the opportunity for local residents to provide their feedback and concerns. This kind of sustained public engagement provides reassurance to constituents, demonstrates a commitment to accountability, and can make a department aware of privacy or transparency concerns that it had not previously considered.

03 Community

Accountability

Emerging technologies give a police department the opportunity to more closely and accurately monitor its own activity. Body-worn cameras have gained the most attention, but data collections of all kinds–from videos of interrogations to datasets of arrest information–give departments, the public, advocacy groups, and academics the opportunity to more closely monitor police officer and staff behavior. Public reports and compliance with public record requests serve everyone's interests.

Public Record Requests
The data collected by many police technologies is subject to public records law. Public record laws encompass digital files, including video, audio, and text files. Even when the data itself is not a public record, information about how that technology is used, such as policies and training material, may be. Compliance with public record laws can be both challenging and expensive in an era of automatic data creation. In addition to responding to public record requests and sending relevant data and files, police departments also need to identify sensitive data and decide what information should be redacted. Depending on the jurisdiction, all license plate reader data or police-worn body camera footage may be subject to public record request laws. The grants that fund the acquisition of this technology often do not extend to cover the public record requests that follow.

Every state has adopted some form of public record law that enables the public to access government files. Public record laws typically allow citizens to obtain copies of government documents that are not confidential, do not contain private information, and do not present a security risk.

Public Reports
Police departments have begun creating public-facing annual reports about the use of surveillance technology within their jurisdictions. In many places, local regulations require police departments to issue these reports and post them on the department's website. Creating public reports can be a helpful, proactive practice for police departments seeking to promote community accountability and build public trust. Across jurisdictions, this type of report chronicles how the police department has addressed many of the issues brought up in this toolkit, including:

- Purpose of the police technology
- Overview of how the technology has been used
- Operating policies
- Policies for data collection, protection, retention, access, and sharing
- Training protocols
- Auditing results
- Impacts on civil liberties and civil rights
- Financial costs
- Records of public meetings and comments from the public

The format and content of the reports vary. For example, the 2018 Seattle Police Department's Automated License Plate Recognition Report is forty-one pages long and includes descriptions of the technology, operating and training policies, and assessments of racial equity and civil liberty concerns. In contrast, police in Davis, CA created a four-page report on GPS monitoring that covered similar issues in a briefer fashion, commenting on training, civil liberties concerns, operating policies, and more.

Community Worksheet: Planning

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help prepare your team.

1. What message do we want to send to our community about this new technology?

2. How can we introduce this new technology in a way that reinforces that message?

3. What are we interested in learning from our community?

4. How will we manage and run our community meetings to make them effective?

Community Worksheet: Planning (Continued)

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help prepare your team.

5. Who will speak on behalf of our department? How can we train or prepare the team for the meeting?

6. How will we communicate operating policies to the community?

7. How will we invite community members to contribute?

8. How will we invite community feedback beyond community meetings?

Community Worksheet: Analysis & Follow-up

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help you process the feedback you received from your community.

1. What concerns has the community raised about the new technology?

2. What misconceptions about this technology need to be addressed?

3. How will we adress these misconceptions?

4. Does the feedback we received affect how we should use this technology? Are there uses of this technology that need to be limited or prohibited?

Community Worksheet: Analysis & Follow-up (Continued)

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help you process the feedback you received from your community.

5. How will we communicate operating policies to our community and the larger public?

6. How will our community and the larger public be able to verify that our department is following these policies?

7. How else can we address our community's concerns?

8. What public reporting and public record laws apply to this technology? Are we prepared to comply?

Community Checklist

Before acquiring or deploying a new police technology, engage your community. It will build trust, prevent miscommunication, and help you to plan. The following checklist provides ways to engage.

1. Community Meetings

- ☐ Hold community meetings before new technologies are procured and deployed.

2. Open Communication

Invite public comments by any means possible, including:

- ☐ Phone
- ☐ Mail
- ☐ Email
- ☐ Website
- ☐ Social media

3. Transparent Operating Policies

Publish operating policies on the police department's website and include:

- ☐ The purpose of each police technology
- ☐ The allowed uses for each police technology
- ☐ The prohibited uses for each police technology
- ☐ Internal oversight practices

4. Annual Public Reports

Publish annual public reports on police technology on the police department's website and include:

- ☐ The purpose of the police technology
- ☐ An overview of how the technology has been used
- ☐ All operating policies, including for data collection, protection, retention, access, and sharing
- ☐ Training Protocols
- ☐ Results of any internal or external audits
- ☐ The benefits these technologies bring to law enforcement investigations
- ☐ The impact on civil liberties
- ☐ The impact on racial, ethnic, and religious equality
- ☐ The fiscal costs
- ☐ The records of public meetings and comments from the public

Conclusion

Police departments across the country face the challenge of properly managing police technology. Modern technology is different than police equipment of the past because of its capacity to acquire, create, store, and interpret data. Modern police technologies can assist with building investigations and deterring criminal activity, but they also carry costs and risks. Police departments are buying data systems, not just hardware. Predicting future expenses is a challenge when data storage and public record requests have limitless potential. Protecting troves of data requires much more sophistication and effort than a strong computer password. And building community relationships is a particular challenge in a time of increased data collection and reduced privacy.

As chronicled in this toolkit, many of the mistakes of police technologies deployment are the direct result of departments not understanding the difference that data makes. We hope that this toolkit provides useful frameworks and worksheets for thinking through modern police technology's unique challenges.

Appendix: Collected Worksheets & Checklists

Police Chief Worksheet

Before purchasing any new technology, consider these big picture questions.

1. Why does my department need this technology?

2. What public safety problem(s) does this technology help solve?

3. Is this public safety problem a priority or a distraction from more important issues in our community?

4. What is the full capacity of this technology—in other words, what does it do and what kinds of data does it collect beyond my organization's needs?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

5. Does the purchase of this technology require approval from legislative bodies, boards, or commissions?

6. What control will my department have over the data that is collected? Who will own it?

7. Who will have access to the data?

8. What are the privacy implications of this technology?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

9. What kind of legal liability could this technology bring?

10. How will my department protect data we collect?

11. How might this technology change my department's relationship with the community? How will deploying this technology affect my officers' day-to-day interactions with our community?

12. What concerns might the public have?

Police Chief Worksheet (Continued)

Before purchasing any new technology, consider these big picture questions.

13. How will my department listen to the public about this technology?

14. What independent research has been done to evaluate this technology? (Independent research is not paid for by developers or vendors of the technology or their agents.)

15. How has this technology worked out in other jurisdictions?

16. How much will it cost? Consider: hardware, software, maintenance, data storage, data security, staffing, training, and compliance with open record laws and policies.

Costs Worksheet

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

1. Are there ongoing costs associated with maintaining the technology or storage equipment? What are the typical costs for a department of our size?

2. Does the vendor provide assistance with transition from older systems? What about transitioning away from the technology if we change vendors in the future?

3. Does the vendor provide training? Does this training fit the needs of our police department?

4. How much does the training cost? How much time does the training take?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

5. Does this technology rely on a proprietary (secret) software that is inaccessible to the police or the public? Are there alternatives available?

6. Has there been any litigation over the use of the technology, either against the company or against a police department that uses the technology?

7. Can our police department control what types of data are collected?

8. Can our police department control who has access to the data collected and can it share it with other entities?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

9. Where is the data we collect stored?

10. Is the vendor prohibited from using, sharing, or selling the data without express permission of our police department?

11. Does the vendor provide security software with this product? Does the software meet the security standards of our state, municipality, and department?

12. Does the vendor use data collected by the police or collect data beyond the needs of law enforcement? If so, how is the company using that data?

Costs Worksheet (Continued)

Calculating the costs and benefits of data-generating technologies is difficult. The following questions make the process more manageable.

13. Have independent studies been conducted on the effectiveness of the technology? (Independent studies are those not conducted or paid for by developers or vendors of the technology or their agents.)

14. Does our department need to sign a non-disclosure agreement to acquire the technology?

Governance Worksheet

When a police department collects data, it must be able to articulate every aspect of its data governance and management plans. These questions are some of the most important to answer.

1. What type of data will we collect?

2. Why do we need this data?

3. How will we use this data?

4. Could this data be used in ways that might raise concerns for our community?

Governance Worksheet (Continued)

When a police department collects data, it must be able to articulate every aspect of its data governance and management plans. These questions are some of the most important to answer.

5. Who in our department will be able to access this data and when?

6. Who will we share this data with?

7. When will we delete this data?

Governance Checklist

Use this checklist to make sure you're covering the most important aspects of your data governance and management plans.

1. Dataset integration

Police departments collect many kinds of data. Although individual datasets may be benign, problems may emerge when coupled with other datasets. Consider, for example, that each dataset may contain information about a piece of a person's life. As datasets become linked, they will form a more complete profile of that person. Dataset integration may make for effective policing, but it also raises increased privacy concerns.

- ☐ Avoid data integration if it is not absolutely necessary for legitimate law enforcement purposes.

2. Security Protocol

For a sample security policy, see the FBI's Criminal Justice Information Services ("CJIS") Security Policy. For a general introduction to institutional data security, see the U.S. Department of Homeland Security Computer Emergency Readiness Team ("US-CERT") security publications. More guidelines can be found at the National Institute of Standards and Technology ("NIST") Computer Security Resource Center.

Include these security protocol basics to ensure your data is secure:

- ☐ Strong password protocol and standards for all devices
- ☐ Effective antivirus and malware software and policies
- ☐ Stringent, limited access policies
- ☐ Limited connection to the internet
- ☐ Frequent purges to eliminate former users

3. Training

In order to keep data secure, reduce employee errors, and help keep staff accountable, your department should incorporate the following two tiers of training:

- ☐ Tier One Training: all employees receive training focused on best practices and spotting common security risks
- ☐ Tier Two Training: employees who work directly with sensitive data, and have the capability to add, delete, alter, or share this data, receive specialized security training

4. Limited access

- ☐ Make sure only personnel who absolutely need data–especially sensitive data–have access to it.
- ☐ Maintain a comprehensive inventory of personnel who have access to sensitive data.
- ☐ Monitor and audit user access to sensitive data.

Governance Checklist (Continued)

Use this checklist to make sure you're covering the most important aspects of your data governance and management plans.

5. Data Sharing

- ☐ Keep track of who we share data with and why.
- ☐ Frequently review whether those we share data with still need it.
- ☐ Vet the organizations we plan to share data with to make sure they have adequate security policies and practices.

6. Data Retention

- ☐ Decide whether automatic or manual deletion approaches are best for each dataset your department collects.

7. Audits

Third-party audits are necessary to protect police data adequately. Some security loopholes escape even the most competent computer users.

- ☐ Use third party auditors to verify that what appears secure is actually secure.

Community Worksheet: Planning

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help prepare your team.

1. What message do we want to send to our community about this new technology?

2. How can we introduce this new technology in a way that reinforces that message?

3. What are we interested in learning from our community?

4. How will we manage and run our community meetings to make them effective?

Community Worksheet: Planning (Continued)

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help prepare your team.

5. Who will speak on behalf of our department? How can we train or prepare the team for the meeting?

6. How will we communicate operating policies to the community?

7. How will we invite community members to contribute?

8. How will we invite community feedback beyond community meetings?

Community Worksheet: Analysis & Follow-up

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help you process the feedback you received from your community.

1. What concerns has the community raised about the new technology?

2. What misconceptions about this technology need to be addressed?

3. How will we adress these misconceptions?

4. Does the feedback we received affect how we should use this technology? Are there uses of this technology that need to be limited or prohibited?

Community Worksheet: Analysis & Follow-up (Continued)

Before acquiring or deploying a new police technology, engage your community to build trust and prevent miscommunication. These questions help you process the feedback you received from your community.

5. How will we communicate operating policies to our community and the larger public?

6. How will our community and the larger public be able to verify that our department is following these policies?

7. How else can we address our community's concerns?

8. What public reporting and public record laws apply to this technology? Are we prepared to comply?

Community Checklist

Before acquiring or deploying a new police technology, engage your community. It will build trust, prevent miscommunication, and help you to plan. The following checklist provides ways to engage.

1. Community Meetings

- ☐ Hold community meetings before new technologies are procured and deployed.

2. Open Communication

Invite public comments by any means possible, including:

- ☐ Phone
- ☐ Mail
- ☐ Email
- ☐ Website
- ☐ Social media

3. Transparent Operating Policies

Publish operating policies on the police department's website and include:

- ☐ The purpose of each police technology
- ☐ The allowed uses for each police technology
- ☐ The prohibited uses for each police technology
- ☐ Internal oversight practices

4. Annual Public Reports

Publish annual public reports on police technology on the police department's website and include:

- ☐ The purpose of the police technology
- ☐ An overview of how the technology has been used
- ☐ All operating policies, including for data collection, protection, retention, access, and sharing
- ☐ Training Protocols
- ☐ Results of any internal or external audits
- ☐ The benefits these technologies bring to law enforcement investigations
- ☐ The impact on civil liberties
- ☐ The impact on racial, ethnic, and religious equality
- ☐ The fiscal costs
- ☐ The records of public meetings and comments from the public