Optimizing Public Surveillance Systems for Crime Control and Prevention

A Guide for Law Enforcement and Their Municipal Partners

February 2020

Rochisha Shukla
URBAN INSTITUTE

Daniel S. Lawrence
URBAN INSTITUTE

Bryce E. Peterson
URBAN INSTITUTE

David McClure
POLICE EXECUTIVE RESEARCH FORUM
This project was supported by Award No. 2015-R2-CX-K002, awarded by the US Department of Justice, Office of Justice Programs, National Institute of Justice. The views expressed here are those of the authors and should not be attributed to the US Department of Justice, the Urban Institute, its trustees, or its funders. Funders do not determine research findings or the insights and recommendations of Urban experts. Further information on the Urban Institute’s funding principles is available at urban.org/fundingprinciples. We would like to thank staff from the Milwaukee Police Department, especially Sgt. Adam Grochowski, who played a significant role working with the researchers for this study. We would also like to thank Nancy La Vigne from the Urban Institute for reviewing and providing valuable feedback on this guide.

# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>STEP 1</td>
<td>Review Current Infrastructure and Define Surveillance Goals</td>
<td>2</td>
</tr>
<tr>
<td>STEP 2</td>
<td>Understand and Develop Policies and Practices</td>
<td>3</td>
</tr>
<tr>
<td>STEP 3</td>
<td>Identify Focus Areas and Incorporate Community Voice</td>
<td>4</td>
</tr>
<tr>
<td>STEP 4</td>
<td>Assess System Performance</td>
<td>5</td>
</tr>
<tr>
<td>STEP 5</td>
<td>Plan to Overcome Constraints</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Camera Features</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Common Surveillance Cameras</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Automation, Video Analytics, and Integration</td>
<td>8</td>
</tr>
<tr>
<td>STEP 6</td>
<td>Acquire the Right Solution</td>
<td>9</td>
</tr>
<tr>
<td>STEP 7</td>
<td>Implement and Maintain the Program</td>
<td>10</td>
</tr>
<tr>
<td>STEP 8</td>
<td>Continue Monitoring the System for Optimal Performance</td>
<td>11</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>REFERENCES</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>ABOUT THE AUTHORS</td>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>
In 2007, only 13 percent of US law enforcement agencies reported having one or more surveillance cameras permanently mounted in a public area, partly because surveillance programs require substantial time and resources (DOJ 2011). The Office of Community Oriented Policing Services published a guide in 2006 exploring early public surveillance systems’ effectiveness and addressing constitutional and privacy concerns about the programs (Ratcliffe 2006); it also developed a guide with the Urban Institute in 2011 to help law enforcement agencies implementing or expanding fixed-camera surveillance programs (La Vigne, Lowry, Dwyer, et al. 2011). The three-city evaluation that informed the 2011 guide concluded that surveillance cameras can reduce crime and be cost-beneficial, but that they are most effective when implemented in areas with historically high crime rates; integrated with other law enforcement systems, technologies, and activities; and monitored in real time by trained personnel (La Vigne, Lowry, Markman, et al. 2011). That guide can still help law enforcement think about what surveillance systems should achieve and problems they may raise. It also considered how agencies could capitalize on costly camera programs, place cameras effectively, and integrate them with complementary technologies.

By 2013, nearly 60 percent of law enforcement agencies reported having some form of video surveillance in public areas, and most agencies in large cities have invested in surveillance systems (DOJ 2015). Despite the systems’ rising popularity, questions remain about how to maximize their efficacy. In particular, developments in video surveillance technology—including automatic license plate readers (ALPRs), facial recognition analytics, and high-resolution cameras—could help agencies make the most of existing systems and improve public safety without investing in monitoring personnel. Still, these advancements are most effective when designed and implemented thoughtfully.

To that end, this guide outlines eight steps for maximizing public surveillance programs’ impact on crime control and prevention. Though it discusses new surveillance technologies available to law enforcement, it focuses on the steps decisionmakers can take and questions they can consider to optimize their surveillance systems. It can also help agencies identify surveillance goals, consider their systems’ limitations and constraints, and develop strategies for meaningful improvements.

WHAT IS THE BASIS FOR THIS GUIDANCE?

This guide draws on a review of evidence-based research, reference materials, and a 2018 project that aimed to optimize the Milwaukee Police Department’s public surveillance system. For that project, the Milwaukee police partnered with the Urban Institute to identify how to improve its camera program, use best practices to develop and implement improvements, and assess these improvements’ impacts on crime and public safety. Urban also interviewed Milwaukee stakeholders who worked within the camera program or routinely used its footage in their work, including camera operators, program supervisors, shift commanders, crash reconstruction unit officers, specialized investigations division officers, criminal investigations bureau detectives, and civilian managers from the department’s communication division.
STEP 1

Review Current Infrastructure and Define Surveillance Goals

Departments should begin improving their surveillance systems by reviewing existing infrastructures for gaps and weaknesses. For example, many surveillance programs have antiquated cameras, limited coverage and viewsheds, and otherwise slow or outdated software and hardware (e.g., operating systems, servers, and cabling). When reviewing their systems, departments should remember that surveillance programs include more than networks of cameras; they can also pull and use data from other technologies (e.g., gunshot detection and ALPRs). It is therefore critical to review all system components, as well as other technologies that could be integrated with broader surveillance programs.

It is also important to define goals for improved surveillance programs. Most police departments use public surveillance cameras to deter criminal behavior and aid investigations. However, departments should tailor their goals to specific needs. For example, decisionmakers may want to use their surveillance program to combat particular types of crime (e.g., violent crimes, auto thefts) or make particular areas safer.

Defining goals up front will ensure surveillance upgrades target specific needs. Otherwise, departments may acquire technologies that, despite having promising applications, do not solve problems specific to their jurisdictions. For example, an agency might purchase increasingly popular facial recognition software without fully considering whether this technology would actually improve public safety. Solutions should always be driven by clearly defined problems (not the other way around).

Similarly, departments defining goals should consider how they will use their surveillance systems. The three main surveillance types (active, passive, and tactical) have different costs, levels of utility, and operations. They can be combined or alternated and have unique trade-offs. For example, tactical surveillance can produce valuable investigative information, but it requires significant coordination among stakeholders to implement. Passive surveillance can provide a useful dragnet for unanticipated incidents, but it produces large amounts of uneventful data and surveillance coverage can be limited, yielding little useful information. Active surveillance helps police respond to incidents that might otherwise go unreported but requires substantial time for camera monitoring. Departments clarifying surveillance goals should consider which strategies are feasible given staffing levels and capabilities.

TYPES OF SURVEILLANCE

1. Tactical surveillance. The system is deployed strategically (and temporarily) to provide data about a specific problem. For example, ALPR cameras placed around suspected chop shops could collect evidence for an investigation of vehicle thefts.

2. Passive surveillance. The system records data from monitored locations to aid future field-initiated inquiries. For example, an officer investigating a break-in at a jewelry shop may request the prior night’s footage from nearby cameras to search for evidence and identify witnesses.

3. Active surveillance. The system is monitored in real time to collect information and give assignments to field officers. For example, a control room operator may scan all the cameras in a downtown area to identify suspicious activities or behaviors that are radioed to patrol officers to investigate.
Some people view or rely on technology as a self-contained solution. However, technology is just one part of surveillance. The policies and guidelines governing how users put information into and get information out of surveillance systems are also critical.

Depending on operational objectives and expectations, simply revising departmental policies may achieve some surveillance goals. For example, many departments assign injured officers temporary duties as surveillance operators to ensure well-trained and experienced staff are using the cameras and interpreting footage. However, this could produce high turnover among people monitoring surveillance systems, preventing them from developing expertise and limiting programs’ impacts. Revising departmental policies to identify people who are able to spend more time monitoring cameras could help departments use existing surveillance systems more effectively. As another example, community members are sensitive to privacy protections, and departments should review policies and practices to achieve privacy-related surveillance goals, such as examining how long evidentiary and nonevidentiary footage is retained, who can view it, and the chain of custody of footage. Understanding how officers are applying policies (and whether those policies are effective) can help departments make necessary revisions up front.

To understand how policy revisions could impact surveillance systems, departments should interview stakeholders about their experiences with the cameras, their perspectives, and their expectations of surveillance. These stakeholders should include:

- members of the executive office,
- camera operators (i.e., those who monitor cameras),
- patrol officers,
- investigators and detectives, and
- prosecutors, defense attorneys, and judges.

These groups must share understandings and expectations of surveillance systems to avoid significant and unnecessary burdens. For example, prosecutors, judges, and defense attorneys often need to know who reviewed or archived video evidence, making it critical for departments to document that information and make it reasonably accessible.
STEP 3

Identify Focus Areas and Incorporate Community Voice

Besides the groups listed in step 2, departments should involve community members in surveillance decisions. This builds community trust and buy-in, which make systems more informed and efficient. Engaging communities can also give agencies opportunities to communicate the privacy safeguards they will employ to protect people’s constitutional rights.

First, it is important to identify who new or improved surveillance programs will affect most. This will typically include neighborhoods or businesses most affected by the issues identified in step 1. For example, a department aiming to reduce shootings in its jurisdiction should begin by working with crime analysts or research partners to identify areas with high concentrations of shootings, as well as areas that may yield valuable investigative information (e.g., hospital drop-offs where shooting victims may be deposited or thoroughfares where stolen vehicles are likely to be flagged).

Departments should then seek community members’ perspectives on the areas they selected, the types of surveillance they will deploy, and their reasons for doing so. Surveillance programs are more transparent when departments explain goals to community members and encourage them to weigh in on decisions about how and where to use surveillance. Departments can do this through focus groups with community members, surveys, or participation in community meetings.

External actors can also participate in decisionmaking by providing information a department may have missed. For instance, residents may desire more surveillance in areas the police had not considered (e.g., areas where crimes are underreported). They may also have ideas about surveillance that could make a department’s solutions more efficient.

Giving community members a voice in these decisions can improve public perceptions of police departments. Research shows that the public’s satisfaction with the police depends not only on crime rates and public disorder, but also on how officers and departments interact with community members (Bradford 2014; Hinds and Murphy 2007; Mazerolle et al. 2013; Reisig, Bratton, and Gertz 2007; Tyler and Wakslak 2004; Wells 2007). In the long run, communities that view the police favorably are more likely to trust and cooperate with its initiatives.
STEP 4
Assess System Performance

In addition to identifying existing departmental policies and focus areas, it is also valuable to understand how existing systems are performing. To accomplish this, departments should build on information collected in the first three steps to identify performance measures relevant to their stated goals. For example, departments aiming to reduce shootings must collect information on when and where shootings occur, what data and systems are available there (e.g., surveillance cameras, gunshot detection, facial recognition, ALPRs), and how often these systems produce useful evidence (e.g., footage of suspects, detected gunshots that alert police, positive identification from facial recognition, captured license plates).

Building out these performance measures provides benchmarks for evaluating improvements to surveillance programs. It will also enable departments to identify gaps in collected data. For example, a department may realize that not linking ALPRs to its record management system makes it difficult to track how often “hits” on stolen or flagged license plates produce useful evidence or facilitate arrests.

After a department has identified relevant performance measures, it can determine the components it needs to bolster. For example, a department aiming to reduce shootings may consider what information it does and does not capture during investigations. This can reveal information the department is missing, such as who shooters are, how many there are, where they come from and where they go, when and where shootings occur, who has been shot, and where victims come from and go. A department may also find that cameras covering areas with high shooting rates have resolutions too low to produce usable footage, and that increasing the resolution would require both higher-resolution cameras and bandwidth beyond the current server’s capacity. Once a department determines such gaps and system constraints, it can better focus on why its system is underperforming and how it can be improved.
STEP 5
Plan to Overcome Constraints

In this step, departments should determine how to address knowledge gaps and system constraints. Solutions can be simple and nontechnical, such as reorienting cameras or removing visual blockades (e.g., tree branches), relocating cameras to areas that need surveillance most, and modifying departmental practices and policies to use existing surveillance systems better. However, newly identified goals may warrant more complicated and technological improvements, such as new cameras, network upgrades, or video analytics. But new technologies also have technical details departments must be familiar with, and it can therefore be helpful to work with independent technical consultants. These experts can review departments’ stated goals, educate them about the latest technologies and best surveillance solutions, and highlight technical details or challenges departments may face.

Camera Features
Cameras have many features departments should consider. These features vary, and include the following:

- **bandwidth**: how much data a camera needs per second to send across a network
- **embedded analytics**: whether a camera performs special processes on images before sending data across a network
- **frames per second**: how many images a camera captures per second to make a video
- **mobility**: whether and how a camera is meant to be used in a fixed location (e.g., a pole-mounted camera), an easily relocated stationary position (e.g., a mobile surveillance station), or a fully mobile position (e.g., a body-worn or vehicle dash–mounted camera)
- **power consumption**: how much energy a camera requires to operate
- **remote control**: whether cameras can scan laterally (pan), scan vertically (tilt), and/or magnify images (zoom)
- **resolution**: the level of detail in images/video footage
- **spectrum**: the type of light a camera captures; this includes light visible to the human eye and parts of the spectrum that are not (e.g., infrared)
- **viewshed**: the area a camera can view at one time
- **zoom**: zooming can be done optically, whereby a camera lens’s physical components move to zoom in or out, or digitally, whereby a computer enlarges an image to increase detail. Resolution is unaffected by optical zoom but greatly affected by digital zoom.
These features are closely related, and changing one can affect the others. For example, cameras with higher resolutions and frames per second typically require more bandwidth to send data across networks. Users can often adjust these features down from maximum values to suit their needs, but purchasing an unnecessarily advanced camera is not an ideal use of resources. Departments should monitor vendors’ installations closely to ensure their cameras’ features are appropriate for departmental needs.

**Common Surveillance Cameras**

Here, we highlight four of the most useful camera types in surveillance hardware.

Departments deciding between these camera types ought to recognize that each has unique benefits and drawbacks, and deploying several types can achieve departmental goals. For example, PTZ cameras can turn to observe specific events within their viewsheds, but this leaves other areas unobserved; panoramic cameras can observe full areas consistently, but they lack PTZ cameras’ high-definition zooming capabilities. Pole camera operators in Milwaukee advised that they prefer to include at least one PTZ camera with each panoramic camera. The panoramic camera gives operators a full, high-definition view of a particular area at all times, and the PTZ camera allows them to examine events in greater detail.

**Pan-tilt-zoom (PTZ) cameras** can typically be controlled by remote operators, programmed to scan an area with preset movements, and/or programmed to move in response to triggering events (e.g., gunshots). They typically have viewsheds of 35 degrees and use optical zooming, though they can also include digital zooming at their maximum optical zoom settings.

**Panoramic cameras** do not move like PTZ cameras but have a wider viewshed (180 degrees or more) that constantly monitors a large area, preventing operators from missing important details when observing something else. They typically have higher resolutions with a single lens, allowing for digital zooming.

**Bullet cameras** are fixed high-definition cameras commonly installed to observe known problem areas in great detail. They cannot pan or tilt, but they allow high-definition zooming.

**Automatic license plate reader cameras** are specifically designed to read license plates. They can use infrared sensors to collect light from reflective materials. They also automatically process images through video analytics software, which confirms whether reflective material is a license plate, identifies characters, and outputs digital versions of license plate numbers that can be stored or cross-referenced against a database.
Automation, Video Analytics, and Integration

Advancements in public surveillance software now allow operators to create complex, preprogrammed touring operations for each camera. A program operator or supervisor determines what areas a camera is most likely to record evidence from when an operator is not monitoring it live. Although this allows departments to collect footage when monitors are unavailable, preprogrammed tours may miss events of interest when rotating or viewing the opposite direction. Users can program cameras to recognize where to look and for how long, when to zoom in, and when to connect with another camera to prevent blind spots. Touring becomes more complicated when different users can program tours based on their preferences. Moreover, when a department identifies a problem in a specific location, it should consider whether and how touring will aid its operations.

Departments must also consider whether to incorporate video analytics into public surveillance systems. Video analytics includes many things and is constantly advancing, creating new applications for law enforcement. Common uses of video analytics include the following:

- **Automatic license plate recognition.** This allows systems to search department lists of wanted vehicles and program cameras to recognize particular plates. This could include vehicles known to be stolen, those known to be involved in felony offenses, and those known to be connected to wanted people. When a camera identifies a relevant license plate, the operator receives an alert on their screen informing them to follow up by, for example, radioing nearby officers to tell them about the car.

- **Connecting to gunshot detection technology.** Pan-tilt-zoom cameras will automatically pan to a predetermined location or a shooting location when an alert from gunshot detection technology is registered within a specific distance of a camera.

- **Crowd detection.** Police use this to prevent groups of people from gathering in particular areas.

- **Facial recognition.** This allows camera systems to recognize human faces and run images through databases to identify people. Law enforcement can connect facial recognition software to records of arrests, criminal histories, and warrants to automatically alert operators when a camera identifies a known suspect.

- **Object detection.** Operators are alerted when an object (such as a bag) is in an area where it would not typically be.

- **Perimeter detection.** Camera operators are alerted when a person or object crosses a predetermined border (for example, someone scaling a fence or going onto a train track).

- **Person tracking.** Although more common in internal surveillance systems, this allows operators to identify a person to track from feed to feed. This spares operators from having to manually change cameras to observe the person’s behaviors.

Most of these analytics (except gunshot detection technology) use cameras that are always fixed on a single frame. This is because video analytics’ algorithms are based on shifts or changes in individual pixels, and video analytic technology is currently incapable of handling the changes that occur when a camera pans, tilts, or zooms.
STEP 6

Acquire the Right Solution

To maximize the return on state and city governments’ investments, most acquisition processes will need to use competitive bidding. A department must release a request for proposals that details what it is looking for in vendor bids. A good request for proposals provides information detailed enough for vendors to prepare realistic and responsive proposals, while providing vendors enough flexibility to propose creative solutions.

The challenge of providing extensive technical detail is how to give vendors enough technical flexibility to create innovative solutions for collecting the data and developing the information a department needs. If a department can articulate its goals and needs clearly in its request for proposals, vendors may recognize technical solutions it had not considered.

WHAT SHOULD REQUESTS FOR PROPOSALS INCLUDE?

- the department’s type of data network (e.g., wireless, fiber), the network’s organization and locations (e.g., hub and spoke), its potential bandwidth, and its current available bandwidth
- the types and specifications of cameras and analytics already on the network
- the types of information the department wants to develop
- clear constraints that cannot be changed
- power sources and supplies
- available mounting surfaces
- local partners who assist in installation (e.g., public works)
Implement and Maintain the Program

After selecting a vendor, a department installs and integrates the vendor’s proposed technological solution with its existing surveillance system. Vendors need a substantial amount of time to install and test new technologies by, for example, connecting to other data sources, creating new operational policies and procedures, or updating data infrastructures. Again, new technology is rarely a self-contained solution; it is usually one part of a broader solution created when multiple system components interact. If new technology is not properly integrated with an existing system, it will be unlikely to perform as expected, and even less likely to provide the performance improvements that were the basis for its acquisition.

Departments should also contractually require vendors to train key stakeholders (such as first-line system users) to use new system components. Moreover, departments should expect vendors to respond to operators’ questions and make requested changes to improve operation.

How department staff perceive new surveillance programs is also critical to sustainability and success. As outlined in step 1, a department can use active, passive, or tactical surveillance styles, which can all involve drastically different staffing needs. For example, a department may opt for an entirely passive program whereby cameras automatically tour across intersections and investigators call in to the camera program to request footage. Such a program may only need one staff member to receive requests, check footage, and produce files of evidentiary value. A department could also combine active, passive, and tactical approaches, requiring staff to observe live footage 24 hours a day, respond to investigative requests, and monitor video analytic capabilities or tactical operations. Such a system would likely require a large staff to run smoothly.

It is also necessary to plan for regular maintenance and have realistic expectations about when to replace surveillance technology. Technology typically has a limited lifespan because hardware wears out, software becomes obsolete, and naturally occurring events can damage and prematurely destroy equipment. Departments should therefore include their expectations for ongoing maintenance and warranties in contracts with vendors, because technological solutions must continue operating after vendors install them.
STEP 8
Continue Monitoring the System for Optimal Performance

Surveillance camera programs can change as new software is developed, departmental needs shift, and community crime patterns change. Departments can best identify and adapt to these changes when they monitor the performance of each component of their surveillance systems. Supervisors can create systematic methods to document instances when camera programs achieve departmental goals, such as when investigators request video evidence, trainings occur, or software is updated.

Collecting data on each system component can help departments locate performance issues. When departments can do so, they can address underperforming components rather than treat whole surveillance programs as single units. Developing a checklist of conditions, considerations, and expected deliverables can make a surveillance system more organized and responsive and simplify an otherwise complex system.

A law enforcement agency may understandably lack the staff needed for in-depth system monitoring. Such an agency could benefit by partnering with outside research organizations that can evaluate its surveillance system’s operations and impact. Many third-party research organizations are dedicated to conducting objective, high-quality research and delivering data-driven policy recommendations and technical assistance for improving policing. These benefits occur through close partnerships, which can require collecting data and interviewing staff and other stakeholders and involve a cost for researchers’ time and effort.
Teams charged with optimizing their law enforcement agencies’ public surveillance programs must consider many factors and should be prepared to become experts on their agencies’ systems. They will need to set program goals by listening to department staff and affected community members to determine what is feasible given existing policies, practices, and infrastructures. After identifying goals, teams will have to understand how their departments’ systems are performing and whether they are meeting those goals. This process will likely surface problems and constraints that will be the focal points of subsequent improvements. Teams will then identify solutions, which might include changing existing systems, installing new cameras, or implementing software enhancements (such as video analytics). Independent technical consultants can help teams identify the technologies most appropriate for departmental goals. (Seeking technical advice from independent consultants rather than vendors is preferable because it is not in a vendor’s interest to highlight surveillance systems’ hidden costs.) Teams will then use competitive bidding to choose vendors to install and integrate the new technologies and train program staff on new software capabilities. Finally, it is crucial that teams monitor their systems for performance issues after making improvements.

A successful surveillance system requires detailed planning, collaborative decisionmaking, strategic investments, and the full integration of public surveillance with agency operations. Carefully following each of this guide’s steps can help agencies upgrade and optimize their surveillance systems to meet surveillance goals.
References


About the Authors

Rochisha Shukla is a research associate in the Justice Policy Center at the Urban Institute, where her research portfolio centers around institutional safety, correctional technology, prison reforms and reentry. Before joining Urban, she completed her master’s degree in criminology and criminal justice from the University of Maryland, College Park. She also holds a bachelor’s degree with honors in psychology and a master’s degree in psychology from the University of Delhi, India.

Daniel S. Lawrence is a principal research associate in the Justice Policy Center. His research focuses on police legitimacy and procedural justice, police technology, police screening and hiring practices, and community policing. He holds a BS in criminal justice from Northeastern University and an MA and PhD in criminology, law, and justice from the University of Illinois at Chicago. He was a coprincipal investigator on this project.

Bryce E. Peterson is a principal research associate in the Justice Policy Center. His research focuses on correctional policy, children of justice-involved parents, prison population forecasting, and technological interventions in criminal justice settings. He received his PhD in criminal justice from the John Jay College/The Graduate Center, City University of New York. He was a coprincipal investigator on this project.

Dave McClure is a senior research associate at the Police Executive Research Forum in Washington, D.C. and was previously a research associate at the Urban Institute’s Justice Policy Center. He has been working in different research, policy, and practice settings to improve the effectiveness and efficiency of justice systems through empirical research, science, and technology. He earned Bachelor’s degrees from the University of Georgia, and his Master’s and Doctoral degrees from George Mason University.