AMERICAN CIVIL
LIBERTIES UNION OF
WASHINGTON
FOUNDATION
901 5TH AVENUE, SUITE 630
SEATTLE, WA 98164
T/206.624.2184
WWW.ACLU-WA.ORG

REGULATING SURVEILLANCE TECHNOLOGY: A TOOLKIT FOR LAWMAKERS

Table of Contents

OVERVIEW

Spurred partly by federal government grants, many local agencies are interested in acquiring and employing new surveillance equipment. While technological advances provide many new capabilities to government, they also have the ability to significantly infringe on privacy and freedom of association rights.

But too often, the impact of surveillance equipment on a community is not fully evaluated before it is put into use. Surveillance equipment can be expensive, and its pros and cons need to be weighed carefully. A formal review and approval process prior to the acquisition and use of new surveillance equipment is essential. It can help to determine whether the technology is indeed necessary and whether its use will promote public safety without unduly compromising privacy or causing other problems.

Government departments should be required to obtain approval from their local legislative body before acquiring new surveillance equipment. To that end, we are providing a model ordinance that requires departments to specify the equipment they wish to acquire and justify its need, along with protocols governing how the equipment will be used, how data will be collected, retained and accessed, and how privacy will be protected.

This toolkit provides lawmakers with the tools they'll need when considering whether to acquire and use surveillance equipment. The toolkit flags issues that should be explored and presents an easy process to evaluate the ramifications of new technologies.

THINGS TO CONSIDER BEFORE ACQUIRING SURVEILLANCE EQUIPMENT

New Technology Can Appear Attractive

Surveillance equipment often appears to be an attractive option for government officials concerned about public safety. Many new technologies can easily capture significant amounts of data, and this information is seen as useful for coping with criminal activity.

BUT Decision-making Should Consider the Complete Picture. A department and elected officials should fully evaluate the actual impact of the equipment and consider the best way to use it. Below we highlight key considerations. Some factors may not be relevant for every piece of technology, and some concerns can be easily addressed with good policy or technology solutions. But it's essential that government leaders look carefully at the full picture before investing in new surveillance devices.

Factors and Concerns for Consideration

- ***Complete Cost.*** New technology often comes with a hefty price tag. It's important to be sure the benefits will outweigh the financial cost. Beyond the initial purchase price, there likely will be significant, ongoing personnel costs and technology expenses to use and maintain the equipment over time.

- ***Effectiveness.*** Will proposed technology actually address the problem at hand? Simply having the ability to capture lots of data does not necessarily mean that criminals will be easier to identify or that crime will be reduced. In some cases, a huge influx of information actually can make it harder to find the truly critical pieces of information. In other cases, the environment in which it is deployed can make even the most advanced equipment less effective than expected. Some cases in point:
    - *Seattle*. In 2008 surveillance cameras were put up in Cal Anderson Park in Seattle in order to address complaints about drug dealing, vandalism and other illegal activity. An audit of the system in 2009 showed that the cameras had not deterred crime in the park and that police had only used the video footage for one criminal investigation.[1] The $850,000 camera system was removed shortly after the audit report proved the investment an expensive waste of valuable public funds.
    - *San Francisco*. A network of cameras installed around San Francisco's public housing developments proved ineffective at aiding in homicide investigations even though approximately one quarter of the city's homicides occurred around public housing. Reasons offered for why the system failed included that the cameras just displaced criminal activity rather than deterring it, and that camera positioning and functionality at night when most crime occurred was not ideal for capturing valuable footage.[2]

---

[1] Seattle Office of the City Auditor, *Cal Anderson Park: Surveillance Camera Pilot Program Evaluation*, October 26, 2009, *available at* http://www.seattle.gov/audit/docs/2009Oct_SurveillanceCamerasHighlights.pdf

[2] Heather Knight, *S.F. public housing cameras no help in homicide arrests*, SF Gate, August 14, 2007, *available at* http://www.sfgate.com/news/article/S-F-public-housing-cameras-no-help-in-homicide-2510907.php%23page-1#page-1

- *Philadelphia*. A Temple University study of the CCTV camera system employed by the City of the Philadelphia found that the cameras were only effective at decreasing crime rates and aiding in investigations in certain areas of the city.[3] The report highlighted that surveillance cameras were therefore not the most effective security measure to address crime universally throughout the city.

- ***Privacy Concerns.*** New technology allows the government to collect types and quantities of data that were once difficult to gather. While camera proponents may assert that people have a limited right to privacy when in public, individuals typically consider their everyday routines as their own business. Yet new technology enables government to collect information that gives a much more detailed picture of people's lives – where they go, what they do, with whom they associate. It's important to consider whether a new piece of equipment allows a new form of tracking that compromises personal privacy. Will use of the technology be problematic for innocent people whose actions it records?

- ***System Misuse.*** Equipment that monitors and collects information about the general public can always be misused by individuals who employ it. People with access to the data may use it for personal reasons, like tracking an ex-lover or work rival, or to engage in voyeurism. In the United Kingdom for instance, CCTV operators have misused the public camera system to spy on women.[4] The systems may also be abused to discriminate by targeting certain racial or ethnic groups. A British study found that operators of surveillance cameras in the UK trained the cameras to follow black males at disproportionately high rates.

- ***Hacking Threats.*** Digital systems are targets for criminal hackers. Systems that collect and store information on members of the public are a treasure trove for wrongdoers seeking to engage in identity theft and other crimes. In addition, when devices are operated remotely, hackers may be able to break into the communication system and take control of the devices. Last year, researchers at the University of Texas demonstrated that they could successfully hijack a drone and give it new flight commands.[5]

- ***Erosion of Community Trust.*** Understandably, members of the public often react strongly when they learn that new surveillance technologies are in use, especially when there is no advance notice or opportunity to comment. Responses are especially vocal when surveillance technology is used to monitor and record activities that people consider private. This public backlash can lead to erosion of public support for or even distrust in law enforcement. Seattle experienced such a backlash when cameras were installed along Alki Beach in West Seattle without public notice or input. Community residents were outraged when they noticed the cameras and learned

---

[3] Jerry Ratcliffe & Travis Tanguchi, *CCTV Camera Evaluation*, Temple University, February 7, 2008, *available at* http://www.temple.edu/cj/misc/PhilaCCTV.pdf

[4] BBC News, *Peeping tom CCTV worker jailed*, January 13, 2006, *available at* http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4609746.stm

[5] Lorenzo Franceschi-Bicchierai. *GPS Hijacking Catches Feds, Drone Makers Off Guard*, Wired, July 19, 2012, *available at* http://www.wired.com/dangerroom/2012/07/drone-gps-spoof/all/

that these could be positioned to view into private residences. City officials had to halt plans to activate the cameras until guidelines are developed to address the privacy concerns.

- ***Surveillance Data Is Available as Public Records.*** Data collected by digital devices operated by government agencies is subject to disclosure under public records laws. This means that, subject to certain statutory exceptions, any member of the public can seek to review the surveillance records and logs. The information collected can be personal or sensitive. Public access can lead to many unintended uses, such as by attorneys desirous of evidence for divorce cases or stalkers eager for more information about their targets.

- ***Conflicts with State Law.*** State law frequently sets limits on types of information that can be collected or how certain types of information must be handled. In addition there are also state regulations about how and where some information can be collected. The use of new technology can conflict with these regulations and often the state restrictions are not thoroughly considered before new equipment is acquired.

Many Concerns Can Be Addressed with Good Planning and a Public Review Process

When concerns are flagged during a public review process, there is a chance to address them. Problems can be fixed either through technological adjustments, internal policies and training, or it may be determined that acquisition of the technology is not justified.

- ***Technological Fixes.*** Many systems can be modified or designed to assist with or restrict certain uses or activities. For example, system security can be bulked up to help prevent hacking. Auditing measures can be built in to help track who uses the equipment and how they use it. Finally, privacy settings can be added to help blur or limit data order to reduce the collection of personal or sensitive information.

- ***Policy Guidelines.*** Departments should develop thorough policies that outline how surveillance equipment may be used, who has access to the data and for what purposes, and how information will be securely retained, stored and deleted. Equipment users should be trained on how the equipment works and what the use policies are. And there should be remedies in place for policy violations.

- ***Is It Really Necessary?*** Considering that surveillance technology by its very nature collects extensive information about individuals, is there truly a strong public benefit that justifies its acquisition?

HOW AN ORDINANCE CAN HELP

As new equipment becomes available, there should be a process in place to think through the costs and benefits and to address concerns – before public money is spent. A way to guarantee this happens is an ordinance, one requiring departments to create use protocols and obtain approval before purchasing and using new surveillance devices. While government departments certainly do internal reviews and analysis before they buy new technology, a public approval process adds important checks and balances.

A review process is valuable to accomplish the following:

Increase Oversight of Government Surveillance

When the government will monitor members of the public, the surveillance program should be reviewed to see if it is necessary, effective and legal. A review process ensures that there is a real need for the new technology and that it will be used in a way that actually improves community safety. Indeed, a formal public review done by a separate government body is a vital step in any democratic process. Its aims are to:

- ***Ensure the value of the equipment has been fully considered.*** A review process can force government departments to think critically about what they hope to gain from the equipment, how the equipment can best be used, and whether the anticipated benefits will justify the costs.
- ***Confirm the proposed uses are legal.*** Checks and balances should be in place to ensure that the new equipment will be used legally. Creating use plans in advance can help identify ways the proposed technology use may violate laws protecting privacy or freedom of speech and association.
- ***Consider the impact on civil liberties.*** It is also valuable to have the proposal reviewed by a non-law enforcement body that can neutrally assess whether the technology poses any risks for civil liberties.

Provide Notice to the Public and Gain Valuable Input

Communication with the public is important. Members of public have a right to know about new equipment, and in turn they may have information that is valuable for the government.

- ***Provide notice to the public.*** When government departments have to announce publicly that they are seeking to acquire new surveillance equipment and have to justify its need and provide use protocols, community members can contribute meaningfully to policy discussions.
- ***Increase trust in government.*** When government is transparent about its actions, people have a greater sense of trust. People resent their government keeping secrets from them, particularly when those secrets involve collection of personal information.
- ***Use community members as resources.*** Many members of the community have technological expertise and may have useful ideas that could improve the use plans for the new equipment. For example, a community member may know of a better way to encrypt sensitive data, or he may be able to propose valuable use protocols that the department had not incorporated.

- ***Clarify uncertainties in advance.*** Unless carefully crafted, the language of protocols can be subject to differing interpretations. Public input can help identify unclear wording, allowing the government to clarify or adjust the protocols.

Identify Privacy Concerns in Advance

When impacts on privacy are considered before a new piece of equipment is used, many problems can be addressed. And privacy concerns that cannot be adequately addressed with planning and policies need to be identified, so that the need for acquisition can be reconsidered.

- ***Identify problems in advance.*** While proponents of new technology may assert that its use will not be problematic, government leaders should carefully consider how it is likely to work in practice. *Consider the following:*
    - Will the technology collect information from places or situations that people typically think of as private?
    - Does the technology allow the government to collect information that was previously very difficult to collect?
    - Is an entirely new type of information being collected?
    - Can more information be collected and stored than was previously possible?
    - Does the technology allow the government to combine or analyze data in a way that reveals more personal or sensitive information?
- ***Come up with ways to address those concerns if possible.*** Asking government agencies to think about how they plan to use new technology before it is acquired and used can allow time to craft workable solutions.
    - Create basic procedures about permitted uses of the technology, how the information will be stored, and who will have access to the data.
    - If good solutions cannot be found, limit the specific uses that will violate civil liberties or restrict the use of the equipment completely.

Identify the Chilling Effects on Speech and Association

New surveillance technologies can allow the government to gather a lot of information about our activities and associations which can have a chilling effect on speech. This is a significant impact that should be addressed before any equipment is acquired and put into use.

- ***Identify whether the technology can interfere with freedom of speech and association.*** Many new pieces of technology collect large volumes of data which seem innocuous in isolation but can create vivid pictures of our lives when combined. It's valuable to identify those capabilities in advance and consider the impact they have on our freedom of speech and association. For example, can the technology capture information that reveals personal relationships or organizational memberships?
- ***Figure out ways to minimize problems, if possible.*** Some speech concerns can be addressed with use, retention and access policies. For example, a policy that provides for regular deletion of information that does not indicate criminal activity could minimize information about personal associations held by the government. If good solutions cannot be found, limit the specific uses that will violate civil liberties or restrict the use of the equipment completely.

A SUMMARY OF THE ORDINANCE

Below is a brief summary of the key components of the model ordinance.

Prior Approval of the Acquisition and Use of Surveillance Equipment and Services

The ordinance requires that government departments receive approval before purchasing new surveillance equipment or before entering into contracts with third parties to provide surveillance services. The ordinance also requires that departments receive approval when they want to use currently owned surveillance equipment in new ways that will provide additional surveillance data. Finally, the ordinance recognizes that updates may be available to currently owned pieces of electronic equipment that would provide surveillance capabilities not previously available to a department. In such circumstances, the department would need prior approval to use the new surveillance capabilities.

Development of Rules and Regulations about Equipment Use and Data Storage

As part of the approval process, a department must submit a set of "operational protocols" and a set of "data management protocols" for council review and approval.

Operational protocols are a set of procedures that will govern how and when the equipment will be used. The operational protocols will include information such as what the purpose of the equipment is, who will be able to operate and access the equipment, where the equipment may be used, and what the standards for use will be.

Data management protocols are a set of procedures that will govern how the data collected by the equipment will be retained, stored, index, accessed and deleted. The data management protocols will include specific information regarding who may access the data and how their access will be tracked, as well as how the information will be secured and deleted to reduce privacy risks.

Public Reporting about the Approval Process

Annually, the council will issue a public report that discloses basic information about how the approval process was used during the year. The report will include information about how many proposals were reviewed throughout the year, as well as how frequently the council approved or denied department requests.

STEPS FOR GETTING THE ORDINANCE PASSED

If you are interested in having an ordinance passed in your jurisdiction, you may want to do one or more of the following:

- **Take stock.** Determine what types of surveillance equipment are currently used in your community and what technology law enforcement is interested in acquiring. (See Appendix A for a list of some surveillance equipment currently available.) This list will help you identify whether you have an immediate need in your community for an ordinance. You also may want to generate a list of surveillance technologies used in surrounding communities. Such a list can highlight the types of issues you may have to deal with in the future. Potential problems may be just as powerful motivators as ongoing issues. In most cases it would be better to have an ordinance in place before issues arise so that you have the tools available to manage the situation.
- **Reach out to colleagues.** Meet with other councilmembers and share this toolkit with them. Determine what will be needed to gain support for the ordinance's passage.
- **Contact the ACLU of Washington.** Reach out to staff at the ACLU of Washington. We may be able to offer you support or advice about introducing and advocating for the passage of the ordinance.
- **Find community allies.** Seek allies in the community who will support and advocate for the ordinance. Identify community organizations, leaders or activists who do work on privacy, government transparency or police accountability and see if they would be interested in supporting the ordinance. Ask them to spread the word with their constituents. Find out if they would be willing to testify in support of the ordinance.
- **Talk with law enforcement.** Set up meetings with law enforcement to discuss the ordinance. Find out what procedures they usually follow when acquiring new technology or what types of procedures and policies they currently have in place for using surveillance equipment. Try to learn what concerns they may have, and discuss workable solutions.

THE MODEL ORDINANCE

BE IT ORDAINED BY THE [_____] AS FOLLOWS:

Section 1. The Council finds that technological advances have provided new equipment that can be used for surveillance purposes. The Council finds that while surveillance equipment may help promote public safety in some contexts, the benefits of such technologies should be balanced with the need to protect privacy and anonymity, free speech and association, and equal protection. The Council finds that the [City/County] should be judicious in its use of surveillance equipment to avoid creating a constant and pervasive surveillance presence in public life. The Council also finds that public review and oversight of new surveillance technologies is fundamental to minimizing the risks posed by such technologies. The Council therefore finds that all [City/County] departments should seek approval from the Council prior to the acquisition and use of certain surveillance equipment and services and should also propose specific protocols for Council review that address how such equipment will be used and how the data it produces will be retained, stored and accessed.

Section 2. The following definitions apply to this Chapter:

(1) "Data management protocols" means procedures governing how data collected by surveillance equipment and services will be retained, stored, indexed, accessed and deleted. Information comprising data management protocols includes, at a minimum, the information required in Section 6.

(2) "Operational protocols" means procedures governing how and when surveillance equipment and services may be used and by whom. Information comprising operational protocols includes, at a minimum, the information required in Section 5.

(3) "Surveillance equipment or services" means:

(a) Electronic, mechanical or other devices capable of systematically collecting, storing and transmitting data, including information, images, videos, photographs or audio, used by or at the direction of a [City/County] department for the purposes of monitoring, observing or analyzing individuals or groups of individuals regardless of whether such data is obscured, de-identified or anonymized before or after collection.

(b) Services provided to a [City/County] department by a third party that result in the acquisition of data, including information, images, video, photographs or audio, by the [City/County] department to be used for the purpose of monitoring, observing or analyzing individuals or groups of individuals regardless of whether such data is obscured, de-identified or anonymized before or after acquisition.

Section 3. Any [City/County] department intending to acquire new surveillance equipment or services shall obtain Council approval via ordinance prior to acquisition. A department seeking to acquire surveillance equipment or services shall submit to the Council a detailed statement of the type of surveillance equipment or services to be acquired along with a set of operational protocols and data management protocols applicable to the use of such surveillance technology or services.

Section 4. Any [City/County] department intending to (a) use previously acquired surveillance equipment or services in a manner or for a purpose not previously disclosed in the operational protocols for such surveillance equipment or services or (b) use previously acquired electronic equipment or third party services in a manner that places such equipment or services within the definition of surveillance equipment or services, shall obtain Council approval via ordinance prior to beginning the new use. A department seeking approval for a new use shall submit to the Council a statement of the new use and a new set of operational protocols and data management protocols for such new use.

Section 5. In requesting approval for the acquisition or new use of surveillance equipment or services, [City/County] departments shall include proposed operational protocols containing the following information for the Council's consideration, along with any other information specifically requested by the Council:

(1) A clear statement describing the purpose and use of the proposed surveillance equipment or services.

(2) The intended specific location of the surveillance equipment if affixed to a building or other structure, or the boundaries of the area where mobile surveillance equipment or services will be used.

(3) How and when a department proposes to use the surveillance equipment or services, such as whether the equipment or services will be operated continuously or used only under specific circumstances, and whether the equipment or services will be installed or used permanently or temporarily.

(4) A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the surveillance equipment or services will be regulated to protect privacy, anonymity, and limit the risk of potential abuse.

(5) The extent to which activity will be monitored in real time as data is being captured and the extent to which monitoring of historically recorded information will occur.

(6) A public outreach plan for each community in which the department intends to use the surveillance equipment or services that provides public disclosure of the new surveillance equipment or the terms of the services agreement and includes opportunity for public meetings, a public comment period, and written agency response to these comments.

(7) If a department intends to share access to the surveillance equipment or services or the collected data with any other government department or entity, it shall set forth which departments or entities are approved for sharing, how such sharing is required for the stated purpose and use of the surveillance equipment or services and the process by which future sharing agreements will be approved by the department and by the Council.

(8) If more than one department will have access to the surveillance equipment or services or collected data, a lead department shall be identified that is responsible for maintaining the equipment or services relationship and ensuring compliance with all related protocols. If the lead department intends to delegate any related responsibilities to other departments or [City/County] personnel, these responsibilities and associated departments and personnel shall be clearly identified.

(9) A plan for maintaining the security and integrity of the surveillance equipment, including an identification of the parties or personnel responsible for the installation or application of hardware and/or software updates and patches, and the procedures by which the lead department will present any substantive changes in the functionality to the Council for approval.

(10) A description of the training to be provided to operators or users of the surveillance equipment or services.

Section 6. In requesting approval for acquisition or new use of surveillance equipment or services, [City/County] departments shall include proposed data management protocols containing the following information for the Council's consideration, along with any other information specifically requested by the Council:

(1) The time period for which any data collected by surveillance equipment or services will be retained.

(2) A description of how and when the data will be retained.

(3) The methods for storing collected data, including how the data is to be labeled or indexed. Such methods must allow for the department personnel and the [City/County] Auditor's Office to

readily search and locate specific data that is collected and determine with certainty that data was properly deleted, consistent with applicable law.

(4) A description of who will have access to the data captured or provided by the surveillance equipment or service, including who will be responsible for authorizing access, who will be allowed to request access, and acceptable reasons for requesting access.

(5) A viewer's log or other comparable method to track viewings of any data captured, collected or provided by the surveillance equipment or services, including the date, time, the individuals involved, and the reason(s) for viewing the records.

(6) A description of the individuals who have authority to obtain copies of the records and how the existence and location of copies will be tracked.

(7) A general description of the system that will be used to store the data.

(8) A description of the unit or individuals responsible for ensuring compliance with Sections 5 and 6 and when and how compliance audits will be conducted.

Section 7. Each [City/County] department operating or using surveillance equipment or services prior to the effective date of this ordinance shall propose written operational protocols consistent with Section 5 and written data management protocols consistent with Section 6 no later than sixty days following the effective date of this ordinance for Council review and approval by ordinance. If Council has not approved or requested modification to the proposed operational and data management protocols within sixty days of their submission to the Council, the [City/County] department shall cease their use of the surveillance equipment or services.

Section 8. Following one year after the effective date of this ordinance, the Council will review its implementation as it applies to [City/County] department use of surveillance equipment or services.

Section 9. Not later than January 15 of each year, the Council shall release a public report containing the following information for the proceeding calendar year:

(1) The number of requests for approval submitted to the Council under this ordinance for the acquisition or new use of surveillance equipment or services.

(2) The number of times the Council approved requests submitted under this ordinance for the acquisition or new use of surveillance equipment or services.

(3) The number of times the Council rejected requests submitted under this ordinance for the acquisition or new use of surveillance equipment or services.

(4) The number of times the Council requested changes be made to operational protocols or data management protocols before approving the acquisition or new use of surveillance equipment or services.

Section 10. Any information obtained using surveillance equipment or services that was not approved in accordance with this ordinance must be deleted as soon as possible, and may not be used, copied, or disclosed for any purpose.

Section 11. Any person who violates the provisions of this ordinance shall be subject to legal action for damages or equitable relief, to be brought by any other person claiming that a violation of this statute has injured his business, his person, or his reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him on account of violation of the provisions of this chapter, and a reasonable attorney's fee and other costs of litigation.

Section 12. Any [City/County] personnel who violates policies contained in this ordinance, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For

[City/County] personnel who are represented under the terms of a collective bargaining agreement, this section prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

APPENDIX A

List of Potential Surveillance Equipment

Automated license plate readers (ALPR)
Audio recorders
Cell phone tracking devices
Fingerprint scanners
GPS tracking devices
Gunshot detectors
Keystroke logging devices
Network sniffers
RFID readers
Stingrays
Thermal imaging devices
Unmanned aerial vehicles (drones)
Video cameras (both fixed and mobile)