

JULY 2019

# TAKE BACK TECH:

## HOW TO EXPOSE AND FIGHT SURVEILLANCE TECH IN YOUR CITY



Photo credit: Grassroots Leadership

---

# INTRODUCTION

In the 21st century, mass incarceration and criminalization have gone high-tech. Today, over 6 million people are under some form of correctional control in the United States. Physical jail cells are being replaced with digital prisons through the expansion of electronic monitoring. More jurisdictions across the country are turning to risk assessment algorithms to grant or deny someone freedom. Data processing companies are helping track and deport immigrants at an unprecedented scale. Add to this reality, facial recognition, drones and other surveillance technologies that are being deployed by local and federal police.

Yet as local and federal police have more and more of these resources, our communities don't really know what is happening, much less the harms to which they're being exposed. Tech is also moving at a significantly faster pace than we have protections in place to stave off the dangers they pose.

Over the last few years, however, cities across the US have begun focusing on regulating how local government, including the police, can purchase and use surveillance technology, how information about residents can be collected, and how it can be shared with other law enforcement agencies, including ICE.

Cities have been pushed to take action by organized communities who have conducted their own research and education, and demanded accountability from their local city and law enforcement agencies. At least 13 jurisdictions including Seattle, Oakland, Santa Clara County, Nashville, Somerville, and Cambridge have passed laws governing the surveillance technology used by their local police departments. Some cities, like St. Louis, are considering whether to pass their own policy.

Big business helps drive the explosion of surveillance technology. Businesses sell surveillance technology to local governments because they profit from these sales. This technology then leads to more policing and incarceration, particularly of Black and brown people. And they're getting away with it - there is very little oversight and transparency over the selling of surveillance technology, and over how it's operating in your city or town. And it doesn't stop there - many of these businesses in the tech industry share data and information with ICE. For example, Vigilant Solutions, a company that collects license plate information from cars had contracts that stated they "owned the data" and could share it with whomever they wanted. And they did, sharing their data with thousands of police departments, as well as with ICE.

We know that every city and every organizing campaign are different. Some organizing efforts have chosen to call for outright bans, others believe that pursuing policy goals to regulate the industry is a tacit acceptance of these technologies, while others have chosen to try regulatory policies as a way to mitigate the harms. Every organized community will have to consider the political conditions and the capacity they have to win their demands. The purpose of this toolkit is to describe the menu of options and pose questions that we can ask ourselves as we approach our cities to ensure that our efforts are helping abolish surveillance and not reinforce it.



Photo credit: Organized Communities Against Deportations

1 "These laws make police get public buy-in on surveillance too," CNET, May 28, 2019, <https://www.cnet.com/news/these-laws-make-police-get-public-buy-in-on-surveillance-tools/>

---

Below are suggested steps for how organized communities can begin the process of researching, educating, and demanding accountability around surveillance and data collection done by their own local governments and police departments.

# ORGANIZER STEPS

## STEP 1

### EDUCATE YOURSELF ABOUT THE TECHNOLOGIES CURRENTLY BEING USED AND THEIR IMPACT

- Do background reading and research
  - Connect with organizations working on policing and surveillance issues
  - Understand which government offices buy surveillance tech
  - Understand some basics about how ICE operates in your city.
- 

## STEP 2

### START THE PROCESS OF COLLECTING THE EVIDENCE FOR YOUR CITY

- Research information that's already been made available by other organizations
  - File a public request to obtain government documents
  - Analyze the government documents to understand the data, tools, tactics being used as well as the companies and government agencies involved
- 

## STEP 3

### USE POLICY ADVOCACY AS A TOOL IN THE FIGHT AGAINST BAD TECH

- Educate and move elected officials to understand the issue with the information and analysis you've provided
- Build enough support to request that elected officials launch their own inquiries
- Consider the range of policy options or solutions that already exist to help inform your demands and local organizing
- Get your local government to pass an anti-surveillance resolution and/or ordinance



# STEP 1

## EDUCATE YOURSELF ABOUT THE TECHNOLOGIES CURRENTLY BEING USED AND THEIR IMPACT

### Background reading and research

The goal is to determine what kinds of surveillance technology your city uses on its residents, how it collects and stores the information, and to what extent the information is shared, including with ICE. Familiarize yourself with surveillance technology and data-collection and sharing. Having a basic understanding of surveillance technology used by local government and how information can be stored and shared will allow you to ask the right questions of your local government.

### Connect with people already engaged in challenging police and surveillance programs

Connect with organizations that combat over-policing and surveillance—mostly criminal justice groups. Some examples of organizations and coalitions working on these issues include:

- [Stop LAPD Spying](#)
- [Oakland Privacy Coalition](#)
- [Black Lives Matter](#)
- or [BYP100](#) coalition spaces

Legal defense communities such as your local public defender, federal public defender or criminal defense attorney offices that may see this surveillance technology or/and information sharing arise in the context of their cases.

Reach out to privacy coalitions. These coalitions often know very little about immigration, and they may feel ambivalent about immigration enforcement. However, they know a lot about surveillance programs.

Connect to organizations that have already filed public records request on surveillance technology (see below).

### Understand which law enforcement divisions in your local government deploy surveillance technology the most.

Some local governments have tech centers that specifically identify themselves as high tech crime solving centers for city or local police departments (e.g. “Real Time Crime Center.”). These centers monitor and surveil communities in real time through the use of surveillance cameras, fixed and mobile license plate recognition (LPR) systems, crime analysis and other law enforcement software and databases. If so, you can make inquiries to local government about their work and their oversight. Do an online search to find out the agencies in your police or local government most engaged with surveillance and data sharing.

Examples:

- [Area Tech Center or Strategic Decision Support Centers, Chicago](#)
- [Real Time Crime Center, Charlotte-Mecklenberg Police Department](#)
- [Real Time Crime Center, St. Louis](#)
- [SeaStat, Seattle Police Department](#)
- [Orlando Police Department Homeland Security Operations Center, Orlando Police Department](#)

#### **TIP**

Here are some materials that can help lay this groundwork:

- [“Who’s Behind ICE?”](#)
- [Blueprint for Terror](#)
- [License Plate Readers](#)
- [Social Media Monitoring](#)
- [Facial Recognition Reports](#)
- [Tech Glossary](#) (see p. 14)

#### **TIP**

Use search terms together like “high tech, crime, police, information sharing, [name of your city]” or research your police department’s web site to learn if these centers exist in your city.



## Understand which law enforcement or local government divisions are in charge of buying surveillance technologies.

As we said earlier, surveillance technology for law enforcement is big business. Identify the office in police and sheriff departments that handles business contracting. (There may or may not be one, depending on the size of your police department.) These offices, often called “procurement offices,” may put out “bids” or “solicitations” to find a business that can fill the need. These offices will vet or help select the company that performs technology or data service. You can learn more about their role from the oversight committee that has jurisdiction over procurements or police.

Examples:

- [Cleveland police](#)
- [Houston police](#) (Go to “business” link)
- [Seattle](#)

### **TIP**

• Good project for a volunteer  
• or an intern!

## Understand some basics about how ICE operates in your city.

Understanding how ICE conducts enforcement in your city will help you understand the connection among surveillance technology, policing and ICE once you start receiving information. For example, the information that the police department collects could be entered into or shared with other databases to which ICE has access.

- Does your city have a 287g agreement or submit to ICE detainees? If so, the city might be sharing personal information about detained immigrants with other law enforcement agencies.
- Does your city get money for renting out bed space in local jails to ICE? If so, the city is getting money from ICE and will likely share personal information about detained immigrants with ICE.
- Does ICE conduct enforcement in the criminal courthouse? If so, the city is likely sharing its criminal court case database in some way with ICE.
- Does your locality have a fusion center? A fusion center is a collaboration made up of local, state, and federal agencies with the purpose of sharing information. If your preliminary research and conversations lead you to believe that local government is directly connected to a fusion center, then there is probably a lot of personal information, like taxes, traffic tickets, and social media information, about residents in your community being shared with the federal government.

Good sources on finding out how police and jails interact with ICE:

- Public defenders
- Court hearings in the local courts
- Immigration attorneys who do majority deportation defense



Illustration: Miguel Lopez

---

## STEP 2 START THE PROCESS OF COLLECTING THE EVIDENCE THAT SHOWS HOW MUCH YOUR LOCAL GOVERNMENT OR POLICE USES SURVEILLANCE TECHNOLOGY

Government agencies at the city, county, state, and federal level buy products and services every day. Local governments in your community spend some amount of their budget purchasing technology-based products and services that expand policing and surveillance under the rationale of improving public safety. These contracts can be tricky to find. There is usually more than one contract or other types of agreements.

You will have to use a variety of tactics to get the policies, contracts or agreements that local governments employ to set up tech surveillance against its residents. This is because police and law enforcement don't want to share this information and think these programs make them more effective. The goal is to get as many documents as you can that relate to the surveillance technology you want to end - a contract, an MOU, a policy, a practice, or a service agreement.

### Research information that's already been made available by other organizations or researchers

If you know the name of the company you want to target or a technology or surveillance program, there are nonprofit organizations that have already filed requests for information for these contracts or services. For example, nearly all the organizations below have filed requests on Palantir Technologies or Vigilant Solutions (license plate readers).

- [Muckrock](#) has filed thousands of FOIA requests and received responses from local governments on surveillance. You can search their files and documents. Use key words like "surveillance and technology and police" or you can run a search based on the name of the company.
- [Electronic Frontier Foundation, Surveillance Technologies](#)
- [Electronic Privacy Information Center Domestic Surveillance project](#):
- [ACLU on Vigilant/license plate readers](#)

#### **TIP**

• Ask a reporter you trust to make inquiries with the police or local government for policies, practices, or agreements on technology surveillance that could be used or deployed by local government or police.

### File an official request to obtain government documents

This is one of the best ways to get as much information as possible about the technology being used against residents. Decide which agencies you want to request information from (your procurement mapping and research into your local surveillance tactics should help you), and what types of technology or information collection you want to focus on. Take a look at the public record act request below to get some names and ideas about what to research and which questions to ask.

- [See our template here or in Appendix B](#)
- Other examples of public records requests:
  - [Police](#)
  - [City Council](#)

---

## Analyze the government documents to understand the data, tools, tactics being used as well as the companies and government agencies involved

Look for a lack of oversight and accountability. Once you've collected the research and information, it's time to analyze the data. Here are some key questions to ask:

- Do the documents you have specifically address immigrants?
- Does the local government pay for these services or the product? For how long?
- Does the local government have civil rights or civil liberties guidelines that the business is required to follow?
- What does the contract(s) allow the business to collect and store? Does the contract or MOU allow the third party business/company to collect pictures of people, cars, and store it? (Sometimes the business negotiates that they will offer a database for free if they are allowed to own the data they collect.)
- Who does the contract allow the data to be shared with?
  - Federal agencies?
  - Other police departments?
  - Other law enforcement agencies? E.g. fusion centers?
- What are the terms for sharing the information
  - Who owns the data?
  - The city?
  - The contractor?
- Which local government office determines that the business is complying with their agreements or complying with civil liberties guidelines?



Photo credit: JUNTOS



---

## STEP 3 USE POLICY ADVOCACY AS A TOOL IN THE FIGHT AGAINST MISUSE AND OVERUSE OF SURVEILLANCE TECHNOLOGY.

### Educate and move elected officials to understand the issue with the information and analysis you've provided

Local governments will need to be educated on the harmful impact of surveillance and data collection on your city's residents. As it stands, cities and towns know very little. Police and local governments often view non-invasive technology (such as videocameras and drones) as being less harmful, even though they facilitate racial profiling and deportation. Also, cities often allow collection of more and more personal information by third parties or share personal information with other law enforcement agencies, like ICE. For example, in a number of states, ICE used facial recognition technology on driver's license pictures after DMVs allowed ICE to access their systems.<sup>2</sup>

### Build enough support to request that elected officials launch their own inquiries

In addition to your research and the results of your public records act request, your local government likely has an oversight committee that can also investigate contracts for surveillance technologies. For example, through them, you might be able to get a list of companies who have agreements or contracts with your local government, including police departments, around surveillance and policing. Getting a local government body to investigate surveillance may serve three purposes: get more information; educate your local government; get local government invested in the issue.

Local government committees that have oversight over procurements and police/public safety contracts or surveillance work could be good targets. The purpose of these committees is to approve contracts or make sure the city or police are not violating laws or policies. Examples of city committees that would have oversight on technology decisions or police:

- [New York City: Committee on Technology has jurisdiction of all technology matters](#)
- [Houston: The technology or public safety committees are good options](#)
- [Denver: Committee on Safety, Housing and Education; no committee on technology, only one for police.](#)

### Consider the range of policy options or solutions that already exist to help inform your demands and local organizing

Once you have educated your local government officials, you may be able to get them to take more aggressive action. Many other localities have already passed resolutions and laws to limit or ban various surveillance practices. Check out the examples linked in this policy chart. New laws and resolutions are being passed every day, so you'll need to do some research when the time comes!

### Get your local government to pass an anti-surveillance resolution and/or ordinance

A resolution spelling out guidelines for cities and towns technology resolution in local government can be a good way to set a baseline about common civil liberties and privacy guidelines. For a local government body that is interested in doing something to support data privacy and limitations on surveillance, but is at the preliminary stages of research and identification of how technology impacts its residents, consider asking the local entity to pass a resolution that sets out topline principles around data privacy and surveillance.

- [See our resolution template here](#) or in Appendix C

If your local government is ready to go further to fight surveillance, you might get it to pass an ordinance or law.

- For some policy ideas to get you started, see the next page.

---

<sup>2</sup> <https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa>

---

# POLICY DEMANDS

Below is a menu of possible ordinance/state law ideas for limiting surveillance. None of these is perfect, and we've tried to spot some of the clear pros and cons for each. As you assemble your policy asks and draft an ordinance, keep your goals in mind. Ask yourself these questions:

## DOES YOUR POLICY/ORDINANCE...

- Reduce funding that goes towards surveillance?
- Challenge the idea that surveillance increases safety?
- Reduce the amount of data and technology that law enforcement (both police and ICE will have at their disposal)?
- Avoid a carve-out for law enforcement agencies/police/prosecutors?
- Give people more control over their data?
- Remove incentives for companies to create more surveillance tech?
- Include an enforcement mechanism that makes it possible for the city and companies to be held accountable if they don't comply with the ordinance?

Remember that you are asking for laws that take powerful tools away from police and that will reduce the profits of powerful companies. You will meet with opposition! Police will say that they need these tools to keep people safe, and companies will invest money and time to keep selling their products and services. **Be prepared for pushback.** Your opponents will try to stop the policy outright or weaken it with exceptions.

As you respond to changes and amendments that lawmakers propose, keep an eye out for these pitfalls:

- Exceptions for law enforcement that allow them to use data or surveillance tech
  - Some arguments for why there should be NO exceptions for law enforcement are:
    - The risks to community members from surveillance outweigh any benefit to law enforcement.
    - Law enforcement already has many tools at their disposal and they don't need these.
    - Time and again, law enforcement has been shown to use these tools in a racially discriminatory or disproportionate manner.
    - Automated License Plate Readers are invasive and give police the power to track anyone's movements -- even though normally they would need a warrant to do the same thing.
    - When facial recognition is paired with the many cameras present in public spaces, it's like asking for people's ID everywhere they go. That's unconstitutional.
  - If despite your best efforts, you're stuck with an exception, you can either decide to withdraw your support from the ordinance, or limit the exception as severely as you can. For example, you could demand that law enforcement agencies have to prove to a neutral body that they are faced with "exigent circumstances" (emergency necessity) that require the use of the tech or the data before the law enforcement agency can use it
- Laws that look good on paper but are hard to enforce
  - If the law can't be enforced, it doesn't really stop the government or companies from spying. The best way to make these laws enforceable is to write them so that regular people can sue for money every time the laws are broken.
  - You can also ask for laws that push for more people than just the attorney general or the city attorney having authority to sue to enforce. Push for enforcement from someone dedicated just to this law and for a way for individuals to petition for enforcement.
  - Push for monetary penalties regardless of the kind of enforcement.
- Striking out in your efforts to stop surveillance? If you can't stop it, slow it down...
  - Can you make the government or a company go through a complicated procedure before they collect data or share data? Can you make that procedure public? Can you make collecting data more expensive? If companies can't make a profit, they are less likely to make the tech and share it with the government.

Categories (brief definitions below; for longer definitions, see Appendix A: Tech Glossary)

- Tech Device Bans
- Limiting Data Collection and/or Sharing
  - Extraction of Data
  - No Local Resources for Immigration Enforcement
  - No Collecting Status Data
  - Consent Requirement
  - Duty of Protection
- Contracting and Investment Policies
- Transparency Policies
- Enforcement Mechanisms

## POLICY DEMANDS (CONTINUED)

**I. Technology Device Bans/Regulations** These have the potential to keep surveillance tech out of the hands of cops, challenge the surveillance as safety narrative, reduce funding for surveillance and reduce incentives to make more surveillance tech!

TYPE	PURPOSE	PROS	CONS
<b>BAN ON CERTAIN SURVEILLANCE TECH</b>	<p>Ban Automated License Plate Readers, facial recognition, and stingrays in public places in your city or town.</p> <p>See <a href="#">Massachusetts Bill</a> and <a href="#">San Francisco Ordinance</a> <a href="#">Somerville</a> re facial recognition, <a href="#">Nashville ordinance</a>.</p> <p>See <a href="#">list of state ALPR policies</a> (none are perfect, but see especially Maine, Montana, and New Hampshire)</p> <p>See <a href="#">Oakland Stingray Policy</a> and <a href="#">South Carolina Cell Site Simulator Ban</a></p>	<p>Harder for DHS to track and arrest people.</p> <p>People not as surveilled in public, which means less data in police hands</p>	<p>Hard to tell what counts as public and hard to enforce.</p> <p>Governments may want a law enforcement exception, so police may still have the tech – if this is the case, try to limit law enforcement use to exigent circumstances or impose some other limit.</p>
<b>BAN ON SALE OF BIOMETRIC DATA</b>	<p>Companies can't sell biometric data, like your facial scan or voiceprints</p> <p>See <a href="#">Illinois Biometric Information Privacy Act</a></p>	<p>Companies would not make as much surveillance tech.</p>	<p>Try to avoid the law being limited to consumers, such as people who use Facebook; try instead for a law that treats biometric data like biological material</p>



Photo credit: JUNTOS



## POLICY DEMANDS (CONTINUED)

**II. Limiting Data Collection & Sharing:** These give people more control over their data and/or limit what the government and corporations can do with data.

TYPE	PURPOSE	PROS	CONS
<b>EXTRACTION</b>	<p>People can remove their data from private and public databases.</p> <p>See <a href="#">California Consumer Protection Act</a> (applies only to private companies)</p>	<p>If data can be extracted or removed, then people's information cannot be shared or used by police or law enforcement.</p> <p>Gives people the most control over their data.</p>	<p>It may be hard to figure out what the exceptions should be (and there should be some exceptions for news &amp; art &amp; where rights of others are involved) .</p> <p>The government will want law enforcement exceptions.</p>
<b>NO LOCAL RESOURCES FOR DHS</b>	<p>No local government resources can go to immigration enforcement or asking about immigration status, including people's time.</p> <p>See <a href="#">California SB 54 Database Guidance</a></p>	<p>Keep local government from cooperating with ICE detainer requests and keep DHS from using local databases for enforcement.</p> <p>More of a sanctuary law, but also reduces surveillance and resources for ICE</p> <p>For more limited version, see below</p>	<p>Government may seek exceptions (for example, California Values Act has carve-outs so that law enforcement can transfer people with certain convictions to ICE custody); could lead to a false sense of security.</p>
<b>STATUS DATA COLLECTION BAN</b>	<p>Local government and companies can't collect data about status</p> <p><a href="#">Santa Ana Sanctuary Ordinance</a> contains a good example</p>	<p>ICE can't access data that's not in the system.</p> <p>People will feel safer using local government services.</p>	<p>Could create a false sense of security.</p> <p>Many law enforcement systems that DHS already uses might be exempt.</p>
<b>CONSENT</b>	<p>Companies and government must tell people how they'll use their data and ask permission for all planned uses when asking people to share info.</p> <p>See <a href="#">California Consumer Protection Act</a> (applies only to private companies)</p>	<p>People can know how companies and the government are using their data.</p> <p>Added barrier to data collection</p>	<p>No one reads the fine print, so people may agree to share their info even when they don't want to, especially if they have to share to get services. Can try to prevent this with rules about plain language.</p> <p>Not as powerful as extraction and doesn't take any resources away from surveillance</p>
<b>PROTECTION</b>	<p>Companies and government responsible for protecting any data they've collected. If the government is responsible for protecting data they collect, then they will have to set up policies or practices to keep the data safe.</p> <p>See <a href="#">EFF on why data fiduciary rules matter</a></p> <p>See <a href="#">Vermont Data Broker Law</a></p>	<p>Anyone harmed by a company or the government failing to protect their data could sue for money.</p> <p>Encourages companies and the government to keep data secure.</p>	<p>May be hard for people suing to show companies or the government at fault.</p> <p>Larger companies will have an easier time complying and being sued and it may make them more powerful.</p> <p>Not as empowering even as consent laws</p>

## POLICY DEMANDS (CONTINUED)

**III. Contracting and Investment Policies:** These policies do less to protect individuals and don't give individuals more power over their data, but they can create accountability, reduce incentives to produce tech or help DHS, and ultimately take resources from DHS.

TYPE	PURPOSE	PROS	CONS
<b>GOVERNMENT CONTRACTING</b>	Local government can't contract with any company that helps DHS enforcement.	Raises awareness and encourages companies not to help DHS.	
<b>PRIVATE CONTRACTING</b>	Local government can't give any benefit (e.g. tax benefit) to any company that helps DHS with enforcement.	Discourage companies from contracting with DHS; make government accountable.	Difficult to enforce
<b>DIVESTMENT</b>	Government must sell its stock in any company that helps DHS enforcement, and can't invest going forward.  See <a href="#">Richmond example</a> (though not as broad as all collaboration)	Same as above	Difficult to enforce

**IV. Transparency Measures:** These don't shift resources or control, but they can slow down data collection and increase awareness. Education can lead to greater support for stronger measures!

TYPE	PURPOSE	PROS	CONS
<b>DISCLOSURE</b>	Government must publish explanation of any new database and get public feedback before setting it up.	Greater public awareness, and makes a record.  Slows down the government when it tries to collect new data or create a new database.	Will also slow the creation of good new systems.  Could make people paranoid instead of inspiring action.  Government will probably want a law enforcement exception.
<b>REVIEW</b>	People can request a copy of their data from the government and private companies  See <a href="#">California Consumer Protection Act</a> (applies only to private companies)	Force companies and government to keep track of people's data.  Increased public awareness.  Force government to come up with a better disclosure system.	Complying with the law will be expensive and the law could hurt smaller companies and make the large companies more powerful.  Complying could take resources from other government programs.  Danger of retaliation.
<b>AUDITS</b>	Neutral review of all government data collection and sharing, contracts, investments, and privacy protections	Increase government transparency. Could also force the government to stay up-to-date with its practices.	Audits are expensive and run the risk of being a rubber stamp.

## POLICY DEMANDS (CONTINUED)

**V. Enforcement Mechanisms:** These enforcement mechanisms can be added on to ensure the proposal can be enforced if the policy is broken! They should be thought of as a part of all of these other potential laws! They're last here only because they apply to everything; they can be just as important as the policy itself.

TYPE	PURPOSE	PROS	CONS
<b>PRIVATE RIGHT OF ACTION</b>	Individuals can sue when a data law is broken, and receive money when they win.	Most enforcement and best option! People don't need to wait for a prosecutor. Companies and/or the government pay the most in penalties and damages.	Likely strong opposition.  Possibly would allow larger companies to kill their smaller competitors by suing them
<b>ESTABLISH DATA GOVERNANCE AGENCY</b>	<p>Create an agency to decide what privacy protections companies and government must use. Agency could also audit the government's data collection, as well as make sure it's not contracting with or investing in companies that help DHS.</p> <p>Agency could take the place of a court and/or could prosecute violations of data laws.</p> <p><a href="#">See Portland</a> and <a href="#">Oakland examples</a></p>	<p>Can make sure community and experts involved in oversight and making policy.</p> <p>More and more expert enforcement than attorney general or city attorney enforcement.</p> <p>Agency enforcement could prevent bad lawsuits meant to kill competition or exploit clients.</p> <p>Could be easier to sue before an agency than in court.</p> <p>Compromise option if you can't get a private right of action.</p>	<p>Very expensive to set up.</p> <p>Could make lawsuits longer and be more expensive.</p> <p>If in charge of enforcement, less enforcement than a private right of action; less empowering.</p>
<b>ATTORNEY GENERAL/CITY ATTORNEY</b>	State attorney general or the city attorney is responsible for enforcing data laws	<p>AG or CA is already set up, so less expensive.</p> <p>Could prevent bad lawsuits meant to kill competition or exploit clients.</p>	<p>Least enforcement, as they enforce many laws. Also the least empowering for individuals.</p> <p>Avoid if possible!</p>



---

# APPENDIX A: TECH GLOSSARY

**Algorithm:** In computer science, an algorithm is a sequence of instructions that a computer program follows. They can be used to calculate driving directions, comparison of prices in online stores, etc. They are most often used in law enforcement to make decisions about people and criminal behavior, mostly if you are a threat. Sometimes these are called “risk-based algorithms” and they can decide whether you get access to bond or not. Sometimes, police use algorithms to see if you are a “risk score.”

**AI:** This is an area of computer science that wants computers to act and think like humans using data that is provided. Machine learning is a core part of AI; it requires the ability to analyze and use huge data sets in short periods of time. The problem is that most of the data that is collected is collected by law enforcement.

**Audits:** Require the local government periodically to review all of its programs that collect PII. The review should ensure that it does not collect more data than absolutely necessary; that it does not retain data longer than necessary; that it employs appropriate measures to protect PII; and that government contractors have not subsequently contracted with DHS

**Automatic License Plate Recognition (ALPR):** It is a system that optically scans vehicle license plates. They are “high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server”, like a database. (From EFF’s “Street Level Surveillance”).

**Ban on certain surveillance technologies:** Prevent any private company and the government from using any form of facial recognition or automated license plate reader technology in any public space. Require anyone using such technology in a private space to obtain consent beforehand. Allow people to sue the government and private companies every time they violate this rule.

**Ban on selling biometric data:** Prevent private companies from profiting by selling, analyzing, or otherwise distributing biometric information, with exceptions for certain services

**Ban on using local government resources to assist in immigration enforcement:** Prevent local government from using any of its financial resources to assist DHS with immigration enforcement, including by asking for or looking up and sharing status information, transferring people to ICE custody, maintaining status-related records

**Biometrics:** The measurement and analysis of unique physical or behavioral characteristics such as fingerprint, face, iris or voice patterns), especially as a means of verifying personal identity. Police collect fingerprints through fingerprints scanners. Facial scans are taken by video cameras in buildings and in public places.

**Cell-site simulators**, also known as Stingrays or international mobile subscriber identity (IMSI) catchers are devices that trick a phone into believing it is a cell-phone tower. Law enforcement uses them to pinpoint a phone to make arrests.

**Consent:** Make companies and the government have a default policy of requiring people to give their consent before companies or the government can collect their personally identifying information (PII). The government and private companies would need to disclose all of the ways in which such data will be used, who will have access to it, and how long it will be stored. Companies and the government should be required to get consent again before using or sharing the data in any new way or keeping it longer.

**Data analytics**, sometimes called big data analytics, is a process of analyzing raw data in order to make conclusions about that information, usually using computer systems and software. Generally, this process collects, organizes and analyzes large sets of data to find patterns, trends or make conclusions. For example, a data analytics company may collect huge amounts of data (raw data) on arrests, race and family information to make predictions about crime or fraud. Data analytics companies will develop predictive policing programs or gang policing tools. This means that they like to collect data or use law enforcement data to make predictions about where crimes are likely to happen. The problem is that most of the “raw data” is collected by law enforcement, not by a neutral party. Palantir is one company in data analytics.

---

## APPENDIX A: TECH GLOSSARY

**Data broker:** A data broker (also called an information reseller, information broker, data aggregator) is a business that collects personal information, public record information, online history, social media, or other information about people and sells that information to other organizations, businesses or law enforcement.

**Data extraction:** Companies may try to “take” data from your phone, computer, or other device through a separate electronic device. Law enforcement often buys these devices. One example of such a device is “Cellebrite,” which breaks into phones and downloads all data from them.

**Data Governance Agency:** Establish a local government agency responsible for setting standards to govern both public and private sectors, including establishing what constitutes reasonable security measures. The agency could also conduct audits, establish procedures to review claims for data violations, and assess local government contracts and investments to prevent DHS collaboration. The agency could also or alternatively review claims as the first step before people sued in court. Alternatively, the local government could create an enforcement branch of the agency to prosecute data violations.

**Data mining:** Data mining is the process of finding patterns and correlations, usually hidden patterns, within large data sets to predict outcomes. Basically, this means that a service digs through huge amounts of data to discover or make connections and predict future outcomes or trends. Most data analytics companies engage in data mining. To do data mining requires that enormous amounts of data be collected.

**Data policing:** This is a term advocates use to describe the way police are using technology to “police” communities.

**Data storage:** Data storage is the storage of information using technology so that it is accessible as needed. Often, technology companies use “cloud storage.” Cloud storage is a way in which data is maintained, managed, backed up remotely and made available to users over the Internet. The consumer (in this case, a city or a law enforcement agency) will pay for their cloud data storage on a per-consumption, monthly rate. This has become big business for companies like Amazon and Microsoft, which provide most cloud storage services to businesses and contractors for DHS and law enforcement.

**Disclosure:** Force local governments to go through a public notice and comment procedure before implementing any new data collection or storage system. Require local government contracts with private companies to be published in unredacted form

**Divestment:** Ban investment in companies that collaborate with DHS and divest any current funds from such companies

**Drones,** also known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UAS), are aircrafts that fly without a pilot aboard. Since drones can fly, they can fly to locations and spy on people, places or objects for law enforcement through windows, etc.

**Extraction:** Allow individuals to remove their data from a private entity’s or the government’s possession, with certain exceptions intended to protect the freedom of expression and important rights of others.

**Facial Recognition:** Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person’s facial contours. Data for facial recognition is collected through video cameras in public places, like parking lots or city streets. Facial recognition is mostly used by police to identify targets or suspects. ICE now possesses facial recognition software. People are very concerned about the overuse of facial recognition.

**Fusion Center:** A domestic “intelligence” gathering center where information is gathered and stored from federal and regional and some law enforcement agencies and civil agencies. There are dozens of fusion centers across the country and they are designed to share information with each other. They hire local, state, federal employees. There is very, very little oversight over fusion centers.

---

## APPENDIX A: TECH GLOSSARY

**Government contracting:** Forbid local governments from contracting with any company that provides any technology or service that enables immigration enforcement and detention unless the local government shows that no reasonable alternative exists

**Immigration-specific collection ban:** Prevent local government and private entities from collecting any information related to immigration status or place of birth (and potentially other categories of sensitive information) unless required by federal law or other compelling reason

**Interoperable databases:** The ability of computer systems or software to exchange and make use of information is what makes a database interoperable with another. Law enforcement uses many databases, but often they cannot connect or communicate with each other. Companies provide services to make these databases communicate with each other so they can share information. The ability of computer systems or software to exchange and make use of information is what makes a database interoperable with another. This allows law enforcement to compare, add or analyze data from one database to another.

**Private contracting:** Ban provision of any local resources, benefits, or incentives for private companies that provide any services to or otherwise contract with DHS for immigration enforcement or detention

**Private Right of Action:** Allow individuals to bring claims for violations of data laws in a court and receive money damages (and possibly civil penalties, or money paid as a punishment) and attorneys' fees

**Protection:** Require entities and the government to keep personal data safe and allow people to sue when they don't. Establish fiduciary (stewardship) relationship of local government and private entities to people whose data they are collecting. Force the government and companies to comply with specific regulations designed to protect individuals' PII.

**Radar devices and equipment:** Law enforcement may use radar devices to monitor or surveil people through these companies. For example, these devices can "see" through walls to see if a person is inside a building.

**Review:** Allow individuals to access a copy of whatever data & categories of data related to them private companies and the government have, without charge.

**Social media monitoring software:** It is common for companies and law enforcement to scan and download social media, like Facebook, WeChat, Twitter, Instagram, YouTube, WhatsApp, or Messenger. This information is sent to police and stored on databases where it can be studied and used by police or ICE. For example, police and ICE often use social media to make assessments about gang involvement.

**Shotspotter** is a system that uses audio sensors to determine when and where shootings take place. The location is then sent to police departments so officers can investigate. That information is sent to a center where a person determines whether it is a gunshot. Then, it is forwarded to police. People use the information collected by shotspotter for data analytics.



---

# APPENDIX B: SAMPLE FOIA

[YOUR ADDRESS]

[DATE]

[ADDRESS]

Re: Public Records Request

To Whom It May Concern:

Requester [NAME ORGANIZATION OR INDIVIDUAL] submits this public records request seeking disclosure of records related to the extent to which [INSERT LOCAL GOVERNMENT, agency, or department] surveils, collects, and shares information on its residents and whether such practices and policies pose civil rights and civil liberties concerns.

I. Government use of surveillance technology

This request seeks the following:

- Any policy directives, guidance documents, orders, memoranda, training materials, user guides, power points, or similar records created after January 1, 2014 containing reference to the use or authorization of surveillance technology as defined in Appendix.
- Any records containing reference to privacy assessments, civil rights or civil liberties, warrant requirements, or/and Fourth Amendment guidance governing the use of surveillance technology.
- Any audits, progress statements, performance assessments, reports containing reference to surveillance technology purchased, licensed, or used by [INSERT LOCAL GOVERNMENT], vendor, or contractor.
- Records dated or created after January 1, 2014 containing reference to the use or purchase of surveillance technology, including but not limited to purchase orders, invoices, RFPs, licensing agreements, documentation of selection, sole source or limited source justification and approval documentation, contracts (including non-disclosure agreements), procurement documents, service or maintenance agreements, memoranda of understanding, and other documentation.
- Budgeting and financial data, spending reports, and cost breakdowns concerning expenditures on any technology related to surveillance technology.
- Records dated or created after January 1, 2014 containing reference to the possible or planned acquisition of surveillance technology.

II. Government contracting with surveillance technology, data broker companies, and/or data storage companies.

- Records dated or created after January 1, 2014 containing reference to the use of data broker companies, as defined in Appendix, including but not limited to purchase orders, invoices, RFPs, licensing agreements, documentation of selection, sole source or limited source justification and approval documentation, contracts (including non-disclosure agreements), procurement documents, service or maintenance agreements, memoranda of understanding, and other documentation.
- Records dated or created after January 1, 2014 containing reference to the use of data storage companies, as defined in Appendix, including but not limited to purchase orders, invoices, RFPs, licensing agreements, documentation of selection, sole source or limited source justification and approval documentation, contracts (including non-disclosure agreements), procurement documents, service or maintenance agreements, memoranda of understanding, and other documentation.
- Records dated or created after January 1, 2014 containing reference to meetings, communications, or follow-up actions with any vendors, companies, or other private entities marketing surveillance technology or data broker company or data storage company services.
- Records dated or created after January 1, 2014 containing reference to how much funding from [INSERT LOCAL GOVERNMENT] is allocated or spent on the purchase, use, or maintenance of surveillance technology and data broker company services.
- Budgeting and financial data, spending reports, and cost breakdowns after January 1, 2014 concerning expenditures on data broker companies.

---

## APPENDIX B: SAMPLE FOIA (CONTINUED)

### III. Government data collection and sharing

- Records containing reference to data collection, storage, retention, and/or data security related to surveillance technology.
- Records containing reference to the name or description of the database(s), network(s) or location(s) where information collected by surveillance technologies is sent or stored.
- Records containing reference to the name or description of the database(s), network(s) or location(s) where images, iris scans, facial scans, fingerprints or other biometric information is stored.
- Records containing reference to any sale, commercial use, or licensing of data collected by or for [local government] to its vendor(s), contractor(s), and/or third parties.
- Records containing reference to any memoranda of understanding, user or login access, licensing, agreement, and/or contract BETWEEN [INSERT LOCAL GOVERNMENT] and/or its vendors or contractors AND any other law enforcement agency regarding access to its data. Other law enforcement agency includes but is not limited to any city, county, or state law enforcement agencies, federal law enforcement agency, and/or fusion centers.
- Records containing reference to any memoranda of understanding, agreement BETWEEN [INSERT LOCAL GOVERNMENT], its agencies, departments, and/or related entities AND any other surveillance technology company, data broker company, and/or data storage company regarding access to its data.
- Budgeting and financial data, spending reports, and cost breakdowns concerning expenditures on facilitating government data sharing after January 1, 2014.

### Application for Waiver or Limitation of Fees

Requester asks for a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and the records are not sought for commercial use.

The request is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the Requester. In the last few years, surveillance technology and data-collection deployed by governments and private companies have raised serious constitutional and privacy concerns.[1] For example, there is widespread concern regarding how surveillance technology companies share information gathered through local government use of their technologies with other government agencies and private companies.[2] There's also deep concern around how much personal data does a local government collect and share with other local or federal government agencies.[3] The records sought are intended to serve the public interest including public education and fostering a larger public discussion on the use of surveillance technology and data collection by governments and private companies and what is the appropriate oversight and accountability mechanism over such surveillance technology and data collection.

[EXPLAIN HOW THE RECORDS SOUGHT WILL BE USED IN THE PUBLIC INTEREST.]

You can reply to this request by contacting [NAME] at [PHONE] or through email at [EMAIL ADDRESS]. You can provide responsive records via email at [EMAIL ADDRESS] or the below mailing address:

[MAILING ADDRESS]

Thank you for your assistance. We look forward to your response.

Sincerely,

\_\_\_\_\_  
[NAME]

---

1 Jack Gillum and Jeff Kao, "Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students", ProPublica, June 25, 2019, available at: <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/>; Crisesider staff, "Does Cellphone Sweeping Stingray Technology Go Too Far," CBS News, November 27, 2017, available: <https://www.cbsnews.com/news/does-cellphone-sweeping-stingray-technology-go-too-far/>; Sahil Chino, "The Racist History Behind Facial Recognition," New York Times, July 10, 2019, <https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html>; Tanvi Misra, "Who's Tracking Your License Plate?" Dec. 2018, available at: <https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904/>.

2 Russell Brandom, "Exclusive: ICE is about to start tracking license plates across the US," The Verge, Jan. 26, 2018, available at: <https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions>; Robert O'Harrow, "DHS 'fusion centers' portrayed as pools of ineptitude and civil liberties intrusions," Washington Post, Oct. 2, 2012, <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html?module=inline>.

3 Bill Chappell, "ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say," NPR, Jul. 8, 2019, available at <https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa>

---

## APPENDIX B: SAMPLE FOIA (CONTINUED)

### APPENDIX

#### Definitions:

1. Surveillance technology includes but is not limited to the following devices and related software and services:
  - Stingrays (IMSI catchers; cell-site simulators)
  - Automatic license plate readers (ALPRs)
  - Closed-circuit television cameras (CCTV; video surveillance)
  - Biometric surveillance technology including but not limited to facial recognition, voice recognition, iris scans, fingerprint scanner technology
  - Gunshot detection and location hardware and services (ShotSpotter, Axon)
  - X-ray vans (Z Backscatter Vans)
  - Surveillance enabled lightbulbs (Surveillance capable bulbs or fixtures)
  - Hacking software or hardware, including phone hacking technology (Cellbrite)
  - Social media monitoring software or SMMS
  - Through-the-wall sensors/radar (TTWS)
  - Police body cameras
  - Predictive policing software or risk assessment algorithms
  - Unmanned aerial vehicles, often refer to as UAVs or drones
  - GPS tracking systems, or location monitoring devices such as ankle monitors.
2. Data Broker company (also commonly called information broker, information reseller, data aggregator, and information solution provider) means a company and/or its software, platform, or services that:
  - Collects information, including identifying information about consumers, from a wide variety of sources for the purposes of reselling such information to their customers, which include both private-sector businesses and government agencies;
  - Collects, repackages, and sells information that is either available in the public domain, or the aggregation of data that was collected for another purpose from that for which it is ultimately used. Known data broker companies include but are not limited to:
    - iAxon
    - Giant Oak
    - Thomson Reuters
    - Palantir
    - Vigilant Solutions
    - PenLink
    - Integrity One Partners
    - Booz Allen
    - Ernst & Young
    - Blue Canopy, powered by Jacobs
    - Motorola
    - Mosaik
    - Deloitte and Touche LLP
    - Procentrix
    - Dun & Bradstreet
    - Cellbrite
    - Magnet forensics
    - Unisys
    - Advance digital forensics
    - Corp Ten International
3. Data storage company means companies that provide the service, software, network and/or platform for storing data including hard drive, server, cloud, and/or other forms of data storage. Known data storage companies include Amazon Web Services, Google, and Microsoft Azure Government.

---

# APPENDIX C: SAMPLE RESOLUTION

WHEREAS the [locality] seeks to affirm and protect the basic human dignity that inheres in every individual who is present in [locality]; and

WHEREAS the [locality] adopts the United Nations finding that privacy is a fundamental human right, and, furthermore, finds that privacy is necessary for the free enjoyment of other fundamental and Constitutional rights, including expression and assembly, and that the welfare of society as a whole requires individual privacy; and

WHEREAS the [locality] finds no aspect of human identity is a commodity, and that appropriation and non-consensual use of any aspect of human identity – including those features deemed “biometrics” – must be avoided except in the most exigent of circumstances; and

WHEREAS the [locality] understands that we live in a rapidly changing world, and that new technologies enable the collection, aggregation, and analysis of many different forms of personal Data such that any Data collection could result in a loss of privacy, and

WHEREAS the [locality] finds that surveillance and monitoring, whether governmental or commercial, deprives individuals of privacy, impinges on important freedoms, dampens human flourishing, and harms society as a whole; and

WHEREAS the [locality] seeks to protect all of its residents regardless of immigration status or any other trait, and seeks especially to protect members of communities that have historically been marginalized, oppressed, or otherwise harmed, especially through use of surveillance and monitoring; and

WHEREAS the [locality] finds that the potential for the distribution of personal Data beyond an individual’s originally contemplated disclosure, for misuse of personal Data, and the grave harms that can stem from such misuse mandate that any entity collecting personal Data, whether governmental or private, first seek the meaningful consent of any individual before collecting personal Data, and thereafter act as a steward of that Data from its collection to its disposal,

BE IT THEREFORE RESOLVED that, in order to fulfill its role of steward of personal Data, [the locality] commits to use of the attached Privacy Principles (Exhibit A) in considering, planning, designing, and implementing any program, project, law, system, or contract that collects, stores, analyzes, or disposes of personal Data; and

BE IT FURTHER RESOLVED that [locality] directs [appropriate local bodies] to identify and develop a process for creating, reviewing, implementing and strengthening equitable and anti-discriminatory policies and procedures that promote these Principles. This will include determining the staff and budget resources needed to implement this process as part of an overall Data Governance strategy for the [locality]; and

BE IT FURTHER RESOLVED, [the locality] directs staff at the [appropriate local bodies] to make recommendations to assure community involvement in the review of City procedures, practices and policies to assure the full and effective implementation of the Principles.

---

## APPENDIX C: SAMPLE RESOLUTION (CONTINUED)

### EXHIBIT A PRIVACY PRINCIPLES

**Transparency and accountability-** [The locality] has an affirmative obligation to publish in an easily accessible manner and in clear terms how the [locality] uses, manages and collects personal Data. [The locality] must also clearly document and publish who creates, contributes to, and has access to that information, including the federal government. Moreover, [the locality] must analyze, document, and publish any potential downstream effects of any contract with a third party (i.e., that party aggregating, selling, sharing, analyzing, or otherwise distributing any personal Data collected for city purposes) and must take measures to protect any personal Data collected by [the locality] from use beyond the originally contemplated and consented to disclosure. [The locality] must work with community stakeholders and experts to establish binding privacy protocols, which it must then publish in an easily accessible manner. [The locality] must conduct regular and frequent audits of all of its Data collection and usage and ensure that its privacy protocols are effective and up to date. [The locality] will contract with experts in this field in conducting audits, analyzing downstream effects, and establishing privacy protocols. When creating any legal regime governing Data, [the locality] will ensure that such laws or ordinances include enforcement mechanisms that permit individuals, and not just government officials, to hold both public and private actors accountable.

**Full lifecycle stewardship** - Data, Metadata and Information will be secured and protected throughout its life cycle. That includes collection, storage, use, control, processing, publication, transfer, retention and disposition.

**Equitable Data management** - [The locality] will prioritize the needs of marginalized communities, including noncitizens, regarding Data and Information management, which must be considered when designing or implementing programs, services, and policies.

**Ethical and non-discriminatory use of Data** - [The locality] has an ethical responsibility to provide good and fair stewardship of Data and Information, following existing non-discriminatory protections, and commits due diligence to understand the impacts of unintended consequences, including the disclosure of Data to the federal government.

**Data openness** - Data, Metadata and Information managed by [the locality] and by third parties working on behalf of the City that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.

**Automated Decision Systems** - [The locality] will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools, including technologies referred to as artificial intelligence, through the lens of equity, fairness, transparency, and accountability. Before adopting any automated decision system, [the locality] will publish its intent and invite public comment, which it will then consider and address before the system can be funded. The Data Governance body established by [the locality] will establish appropriate notice and comment procedures for this purpose.

**Biometric & photographic data** - [The locality] recognizes the especially sensitive nature of biometric information and will audit and publish its use of every system that collects such information, and, prior to adopting any new system that collects such data, first establish that exigent circumstances require its adoption and subject it to the same notice and comment procedure prescribed for the adoption of Automated Decision Systems.

**Data utility** -All Information and Data processes must bring value to [the locality] and the communities [the locality] serves. [The locality] will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.