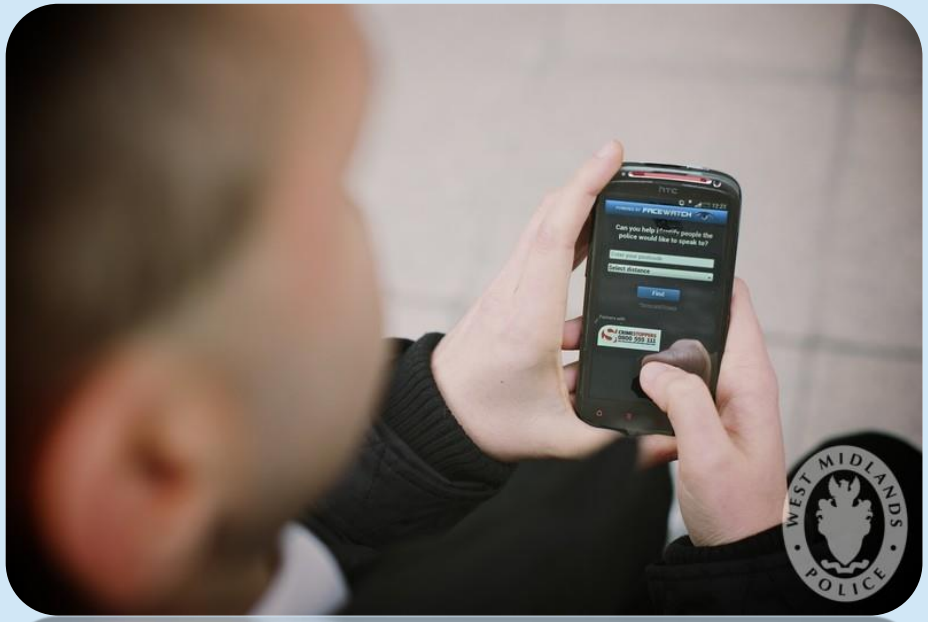
The New Shiny Toy:

Legal and Policy Implications for the Procurement of New Technologies by Police



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

Ronald Davis
Visiting Senior Fellow, Criminal Justice Policy Program
Harvard Law School

Brook Hopkins
Executive Director, Criminal Justice Policy Program
Harvard Law School

www.techandpolicing.org

www.techandpolicing.org

Harvard-Stanford Project on Technology and Policing
Advisory Board

- **Matt Cagle**, Technology and Civil Liberties Policy Attorney, ACLU of Northern California
- **Amy Condon**, Former Legal Advisor, Boston Police Department
- **Catherine Crump**, Assistant Clinical Professor and Director of the Samuelson Law, Technology & Public Policy Clinic Berkeley School of Law
- **Ronald Davis,** Former Director of the Office of Community Oriented Policing Services, U.S. Department of Justice
- **Ifred Durham**, Police Chief, Richmond (VA) Police Department
- **Isaiah Fields**, Associate General Counsel and Vice President of Government Affairs Axon Enterprise, Inc.
- **Andrew Ferguson**, Professor of Law, University of District Columbia School of Law

- **Clare Garvie,** Associate, Center on Privacy & Technology at Georgetown Law
- **Sharad Goel,** Assistant Professor, Department of Management Science & Engineering, Stanford University
- **Elizabeth Joh,** Professor of Law, University of California-Davis

www.techandpolicing.org

- **Venus Johnson,** Director of Public Safety, Office of Oakland Mayor Libby Schaaf
- **Eric Jones,** Police Chief, Stockton (CA) Police Department
- **Nicole Jones,** Senior Law Enforcement & Security Counsel, Google
- **Vivek Krishnamurthy**, Clinical Instructor, Cyberlaw Clinic, Harvard Law School
- **David Roberts**, Director of NCS-X Technical Assistance and Outreach Bureau of Justice Statistics, U.S. Department of Justice, Senior Program Manager, IACP Technology Center
- **Adam Schwartz,** Senior Staff Attorney, Electronic Frontier Foundation
- **Sameena Usman,** Government Relations Coordinator, Council on American-Islamic Relations
- **Reilly Webb,** Deputy Executive Director, Texas Governor Greg Abbott's Criminal Justice Division

Framework for Regulating Police Technology

- Accuracy, Bias, & Accountability
- Privacy
- Community Involvement
- Data Governance

www.techandpolicing.org

Harvard-Stanford Project on Technology and Policing

Procurement Practices Toolkit

Contents

Start by Asking the Right Questions

Most of the policing technologies currently on the market are designed, tested, and marketed by private companies. These companies make decisions about the features, capabilities, and limitations of the technologies police rely on. As a result, private vendors are an important source of information for departments considering acquiring new policing technologies. This section provides guidance for getting the most out of conversations with vendors.

1. The Bigger Picture

Technology vendors are understandably eager to tell police about the benefits of their products. Remember to ask about the potential costs and downsides as well.

Costs should be assessed with the technology's entire lifespan in mind. This means get information not just about the upfront costs of the technology, but also how much departments are likely to spend on training, technical maintenance, and data storage over time.

Getting a vendor to discuss the downsides of their product can be difficult. However, it's still worth asking: a vendor who can't (or won't) answer questions about the technical limitations, potential misuses, or legal status of a piece of technology is a red flag.

> ***The Risk is Real***
>
> In 2015, Boston's ALPR data was stored on a database that was accessible to the public through Google search. In fact, it was the private vendor of the ALPR technology that enabled the breach. The revelation of this breach was costly: both in terms of costs as well as public trust. The lesson to take away from this incident is twofold: data security is essential, and vendors cannot always be trusted to effectively manage all aspects of their product's data governance. After all, it was the city – not the vendor – who was held accountable by the public.

2. Ask About Data Governance

Technology companies make decisions about who owns the data gathered by their technologies and how that data is stored, used, shared, and retained or deleted—activities that are collectively called "data governance." Before procuring a new technology, you need to know which data governance decisions have been made by the vendor and which are left to the department. Some of the ways vendors control data after technology is in the hands of the police include:

- Preventing police departments from disclosing data to the public without prior permission;
- Determining where data is stored, how it is secured, and who can access it;
- Using proprietary (i.e., secret) algorithms to interpret data; and
- Using the data gathered by police departments for private purposes.

This is not to say that all data governance decisions need to be made by police departments. In fact, experts from technology companies may provide sound policies that local police departments can adopt. The point is that departments procuring new technologies must understand any governance practices imposed by private companies and make sure those practices do not conflict with the department's own priorities.

Spotlight: Automated Decision-Making

Automated decision-making technologies are tools designed to supplement—or replace—routine police officer tasks. Current automated decision-making tools include license plate readers that determine whether a car is stolen; facial recognition software that picks a person with an arrest warrant out of a crowd; and predictive policing algorithms that determine whether a person is at risk of committing or being a victim of a crime. At the root of these tools are algorithms: computer processes that do the work people used to do.

Algorithms promise to improve the efficiency of police and free up resources for overworked departments. But as with other technologies, developers are not always open about the limitations of these tools. The delegation of decision-making to software can invite a number of problems: false positive matches, unintended racial biases, computer errors, or even just an unhelpful deluge of data analysis. Whole books are being written about responsible use of algorithms in the law enforcement—far more than we can fit in this guide. Instead, here are some basic principles that you should keep in mind when reviewing technologies that automated decision-making:

Always Confirm Information Before Using It. Automated decision-making tools make mistakes, and sometimes they are mistakes that would be obvious to a person. For example, automated license plate readers occasionally read plates incorrectly—sometimes leading to tense situations. One U.S. Court of Appeals has ruled that reliance on an algorithm without human confirmation can, in some cases, constitute unreasonable police conduct.

If the Vendor Can't Explain It, Don't Use It. Many automated decision-making tools are "black boxes," meaning that users don't know exactly how the decisions are being made. This can present challenges when police have to defend the use of these tools. Only adopt technologies that can generate meaningful explanations—not only is this a best practice, it may soon be required by law in some cities.

Get Evidence of Outcomes. Automated decision-making tools often promise to be less biased and more reliable than humans. In reality, there may not be much difference between the two. Before adopting an automated decision-making tool, look for independent studies that verify its fairness and accuracy.

3. Do Your Homework

After talking to a vendor about their technology, you should take some time to do your own research. There's a good chance that you're not the first person to consider this technology, so you can benefit from others' experiences.

First, you should look to see if the technology you're considering, or the vendor that sells it, has been in the news recently. If a technology is at the center of a public or legal controversy, you want to be very careful before adopting it.

Next, see if any other departments in your area are using the technology. Fellow police may be more upfront than vendors about the benefits and drawbacks of using a particular technology.

Finally, look for any independent academic research regarding the technology. Many popular police technologies have been in use long enough that multi-year, empirical studies about their effectiveness are available. These studies can give you a better idea of what costs and benefits to expect from a technology in real-world conditions.

Worksheet: Questions to Ask Vendors

When interacting with a private vendor, consider this checklist before procuring any new data-gathering technology:

- [ ] Are there ongoing costs associated with maintaining the technology or storing equipment? What are the typical costs for a department of your size?
- [ ] Does the company provide technology training? Does this training fit the needs of the police department? How much does the training cost?
- [ ] Does this technology rely on a proprietary (secret) software that is inaccessible to the police? To the public? Are there alternatives available?
- [ ] Has there been any litigation over the use of the technology, either against the company or against a police department that uses the technology?
- [ ] Can the police department control what types of data are collected?
- [ ] Can the police department control who has access the data collected?
- [ ] Can the police department share the data it gathers with other public entities?
- [ ] Does the company provide security software with this product? Does this security software meet the needs of the police department?

  To get the most out of this question, take a copy of your security policy with you when you meet with vendors.
- [ ] Does the company use data collected by the police or collect data beyond the needs of law enforcement? If so, how is the company using that data?

Draft an Access Policy

An **access policy** is a policy that determines who has access to a dataset, network, or device. It also determines *how much* access each person has. The best access policies require logging all access and activity. Access policies can, if necessary, also restrict which *devices* a certain dataset is accessible on. For example, mobile phones are notoriously unsafe, and it is better to avoid accessing sensitive data on a laptop that is connected to a public wireless network.

Worksheet: Do You Need an Access Policy?

Are you dealing with technology that…

[ ] Records and/or stores audio, video, or photographs?
Common examples: CCTV, ShotSpotters, body cameras, ALPRs

[ ] Records and/or stores location data?
Common examples: "StingRays", GPS tracking devices

[ ] Aggregates and stores public or semi-public information?
Common examples: social media analytics, facial recognition databases

[ ] Otherwise has some sort of software or network that can be logged into?

If the answer to any of the above is "yes," you need an Access Policy.

Three Reasons to Have an Access Policy

1. To Keep Data Safe by Reducing the Possibility of Attack

The fewer points of access into a system, the harder it is to hack into. Put simply, every person who has access to a particular system, network, or database is a potential vector for a cyberattack. If police systems are hacked it can lead to public outcry and loss of confidence in the department. It can also lead to the loss of data, contamination of digital evidence, and significant costs.

The Risk is Real

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

2. To Limit the Risk of Misuse or Abuse

The fewer people who have access to sensitive data, the fewer chances there are for a bad — or simply misguided — party to misuse the information that is available. All it takes is a single officer with a grudge and access to sensitive data to ruin a department's reputation. Less dramatically, the more people who have access, the higher the risk someone will accidently leave a login unattended or otherwise compromise security through carelessness. **Even if you have complete confidence in everyone in your department, limiting access shows that you're taking data security concerns seriously.**

3. To Increase Accountability

Logging all access and use increases accountability and helps with efficient problem solving if things do go wrong. For instance, accurate logs might help you catch and retrain the careless officer who leaves his login open *before* anything bad happens.

The Principle of Least Privilege

The best practice in creating a data policy is the **principle of least privilege.** This principle means that **each person who has access to a dataset or network should only have as much access as they need to do their job.**

Access isn't an all-or-nothing prospect. Just like your IT specialist can probably get to certain administrative functions on your work computer which you are shut off from, different people can be given different levels of data or network access.

For Example…

A dataset could allow officers to search the data, but not alter or delete any of it.

Users can always be granted higher privileges temporarily if necessary for certain projects. The key word there is *temporary*. It may seem simpler to just grant everyone higher privileges rather than dealing with granting temporary privileges, but never forget: **The fewer people who have access, the safer your data is!**

Worksheet: Draft an Access Policy

What different levels of access are currently available?

Are there more detailed levels of access that would better reflect the needs of specific officers (or assignments)?

Most software products allow you to set levels of access other than the defaults.

Does every officer require **some** sort of access to this dataset or network?

[ ] Yes

[ ] No

If yes: Why?

If you have teams that work together, is it possible to have just one point-person per team with access?

If no: Which officers (or assignments) will need access?

Why?

Worksheet: Draft an Access Policy (con't)

Are there other (non-officer) staff members who will require access?

[ ] Yes

[ ] No

If yes: Who, and why?

What is the **lowest** level of access that will allow the average user to do their job?

Are there certain officers (or positions) who will need a higher level of access to do their job?

[ ] Yes

[ ] No

If yes: Who, and why?

Remember: you want as few officer as possible with higher levels of access. Temporary elevated access can always be granted later if needed!

Who absolutely *must* have the highest level of access?

Why?

This is just to help you draft a policy. You should make sure a technology security expert helps you set up the actual system to ensure it complies with your policy.

Harvard-Stanford Project on Technology and Policing

www.techandpolicing.org

info@techandpolicing.org