Q&A: What Philadelphians need to know about the city's 7,000-camera surveillance system

May 27 2024, by Albert Fox Cahn

Credit: Pixabay/CC0 Public Domain
The *Philadelphia Inquirer* recently investigated Philadelphia's use of what it described as a "little-scrutinized, 7,000-camera system that is exposing residents across the city to heightened surveillance with few rules or safeguards against abuse." The article detailed how Philadelphia narcotics cops not only allegedly failed to disclose their use of video surveillance in arrest reports or to prosecutors, but also that the video footage at times proved officers were lying when they testified.

The Conversation U.S. talked to Albert Fox Cahn, founder and executive director of the nonprofit Surveillance Technology Oversight Project and a practitioner-in-residence at NYU School of Law, about what these new video systems can do and the privacy and other issues they raise.

**What can these cameras do?**

The *closed-circuit television*, or CCTV, cameras most Americans pass each day may look interchangeable, but a lot has changed behind the lens in recent years. As video *surveillance* cameras have become cheaper and more ubiquitous, they have also grown more powerful—featuring increasingly high-definition images and the ability to *pan, tilt and zoom*. But the most significant change to cameras like those used in Philadelphia is the networks that police departments set up to aggregate these countless images of city residents' daily lives.

A variety of AI tools can also harvest this data in new ways that some may find alarming.

*Automated license plate reader software* can both track drivers across the city in real time and create a long-term log of their cars' movements. Want to know where a driver is now or was parked two years ago? Just check the database.
And pedestrians are no less prone to surveillance. Facial recognition software can scan images to automatically identify individuals and track them across the city.

How widespread is this technology?

According to the Inquirer's investigation, Philadelphia's camera network grew at an astounding pace. In the past decade, the city has gone from 216 cameras to a network of more than 7,000 cameras operated by police and transportation officials.

But those are just the cameras that city officials directly control and can access in real time.

In addition, police routinely turn to the images captured by private surveillance cameras. This includes everything from multimillion-dollar, internet-enabled camera systems at large stores, offices and universities to the individual cameras that homeowners or small-business owners screw into their door frames or exteriors. The public simply has no idea how many of these private cameras are in operation or how often their data is requested.

How is this different from traditional police video surveillance?

Traditional cameras offered a narrow, grainy perspective on a single fixed place. These systems not only collected much less data than contemporary cameras, but they also retained far less.

A single CCTV camera at a bank might help police identify a suspect in a robbery, but it poses no privacy threat beyond that. It is confined to a small space where privacy concerns are minimal and security concerns
are high. But mass camera deployments create a fundamentally different model, collecting far more information on all of us and creating far greater potential for misuse.

Police have attempted these techniques for decades, but the technology simply wasn't up to the task. When the City of London Police deployed its so-called "ring of steel" security system in the 1990s, fewer than two dozen cameras tried to track the cars entering a tiny portion of the British capital, surveilling roughly a square kilometer of the city's financial core. Officers manually jotted down vehicle plate numbers and surveilled drivers' profile photos.

The labor-intensive exercise was impossible to scale.

To deploy such a system across an entire city would likely have taken every police officer in the city and then some. Through automation, technology enables this mass surveillance by reducing the marginal cost of tracking, allowing police to expand monitoring far more broadly than would have been financially or pragmatically possible before.

**What privacy concerns does it raise?**

A single camera can capture our image; a citywide camera system can reconstruct our lives. Networked camera systems like those in Philadelphia, when combined with smartphones and other internet-enabled devices, allow officers to reconstruct an individual's movements for days or weeks at a time, all without any court oversight.

While it would take a warrant to install a GPS tracker on a resident's car, police can recreate GPS-like location tracking without a warrant, all thanks to mass camera systems. And facial recognition in municipal cameras threatens the First Amendment, which protects freedom of speech, religion and peaceful assembly. The police are armed with a way
to track nearly every person at a political protest, abortion clinic or house of worship. Such surveillance melts away the anonymity that is indispensable to an open society.

**Are there other risks or unintended consequences?**

I believe giving thousands of city employees the keys to a small surveillance state is a recipe for disaster.

The Philadelphia Inquirer found that the city has policies that forbid zooming in on residents for amusement, spying on someone by zooming in through their window, or blatant racial profiling. But what it didn't find was evidence that these safeguards were being enforced.

When thousands of employees can spy on their neighbors, romantic partners and business rivals on a whim, it raises the question: Who watches the watchers?

At least for now, the grim answer appears to be no one.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation
