High-tech surveillance amplifies police bias and overreach
12 June 2020, by Andrew Guthrie Ferguson

Police forces have a wide range of options for monitoring individuals and crowds. Credit: Nicholas Kaeser/Flickr, CC BY-NC

Video of police in riot gear clashing with unarmed protesters in the wake of the killing of George Floyd by Minneapolis police officer Derek Chauvin has filled social media feeds. Meanwhile, police surveillance of protesters has remained largely out of sight.

Local, state and federal law enforcement organizations use an array of surveillance technologies to identify and track protesters, from facial recognition to military-grade drones.

Police use of these national security-style surveillance techniques—justified as cost-effective techniques that avoid human bias and error – has grown hand-in-hand with the increased militarization of law enforcement. Extensive research, including my own, has shown that these expansive and powerful surveillance capabilities have exacerbated rather than reduced bias, overreach and abuse in policing, and they pose a growing threat to civil liberties.

Police reform efforts are increasingly looking at law enforcement organizations’ use of surveillance technologies. In the wake of the current unrest, IBM, Amazon and Microsoft have put the brakes on police use of the companies’ facial recognition technology. And police reform bills submitted by the Democrats in the U.S. House of Representatives call for regulating police use of facial recognition systems.

A decade of big data policing

We haven't always lived in a world of police cameras, smart sensors and predictive analytics. Recession and rage fueled the initial rise of big data policing technologies. In 2009, in the face of federal, state and local budget cuts caused by the Great Recession, police departments began looking for ways to do more with less. Technology companies rushed to fill the gaps, offering new forms of data-driven policing as models of efficiency and cost reduction.

Then, in 2014, the police killing of Michael Brown in Ferguson, Missouri, upended already fraying police and community relationships. The killings of Michael Brown, Eric Garner, Philando Castile, Tamir Rice, Walter Scott, Sandra Bland, Freddie Gray and George Floyd all sparked nationwide protests and calls for racial justice and police reform. Policing was driven into crisis mode as community outrage threatened to delegitimize the existing police power structure.

In response to the twin threats of cost pressures and community criticism, police departments further embraced startup technology companies selling big data efficiencies and the hope that something “data-driven” would allow communities to move beyond the all-too-human problems of policing. Predictive analytics and bodycam video capabilities were sold as objective solutions to racial bias. In large measure, the public relations strategy worked, which has allowed law enforcement to embrace predictive policing and increased digital surveillance.
Today, in the midst of renewed outrage against structural racism and police brutality, and in the shadow of an even deeper economic recession, law enforcement organizations face the same temptation to adopt a technology-based solution to deep societal problems. Police chiefs are likely to want to turn the page from the current levels of community anger and distrust.

The dangers of high-tech surveillance

Instead of repeating the mistakes of the past 12 years or so, communities have an opportunity to reject the expansion of big data policing. The dangers have only increased, the harms made plain by experience.

Those small startup companies that initially rushed into the policing business have been replaced by big technology companies with deep pockets and big ambitions.

Axon capitalized on the demands for police accountability after the protests in Ferguson and Baltimore to become a multimillion dollar company providing digital services for police-worn body cameras. Amazon has been expanding partnerships with hundreds of police departments through its Ring cameras and Neighbors App. Other companies like BriefCam, Palantir and Shotspotter offer a host of video analytics, social network analysis and other sensor technologies with the ability to sell technology cheaply in the short run with the hope for long term market advantage.

The technology itself is more powerful. The algorithmic models created a decade ago pale in comparison to machine learning capabilities today. Video camera streams have been digitized and augmented with analytics and facial recognition capabilities, turning static surveillance into a virtual time machine to find patterns in crowds. Adding to the data trap are smartphones, smart homes and smart cars, which now allow police to uncover individuals’ digital trails with relative ease.

The technology is more interconnected. One of the natural limiting factors of first generation big data policing technology was the fact that it remained siloed. Databases could not communicate with one another. Data could not be easily shared. That limiting factor has shrunk as more aggregated data systems have been developed within government and by private vendors.

The promise of objective, unbiased technology didn’t pan out. Race bias in policing was not fixed by turning on a camera. Instead the technology created new problems, including highlighting the lack of accountability for high-profile instances of police violence.

Lessons for reining in police spying

The harms of big data policing have been repeatedly exposed. Programs that attempted to predict individuals’ behaviors in Chicago and Los Angeles have been shut down after devastating audits cataloged their discriminatory impact and practical failure. Place-based predictive systems have been shut down in Los Angeles and other cities that initially had adopted the technology. Scandals involving facial recognition, social network analysis technology and large-scale sensor surveillance serve as a warning that technology cannot address the deeper issues of race, power and privacy that lie at the heart of modern-day policing.

The lesson of the first era of big data policing is that issues of race, transparency and constitutional rights must be at the forefront of design, regulation and use. Every mistake can be traced to a failure to see how the surveillance technology fits within the context of modern police power—a context that includes longstanding issues of racism and social control. Every solution points to addressing that power imbalance at the front end, through local oversight, community engagement and federal law, not after the technology has been adopted.

The debates about defunding, demilitarizing and reimagining existing law enforcement practices must include a discussion about police surveillance. There are a decade of missteps to learn from and era-defining privacy and racial justice challenges ahead. How police departments respond to the siren call of big data surveillance will reveal whether they’re on course to repeat the same
mistakes.

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