FUTURE TENSE

The Next Frontier of Police Surveillance Is Drones

A major drone company and a major police-camera company are teaming up, and the possibilities are frightening.

By APRIL GLASER
JUNE 07, 2018 • 5:00 PM

DJI's Matrice 200 drone.
DJI

A company that makes stun guns and body cameras is teaming up with a company that makes drones to sell drones to police departments, and that might not even be the most worrisome part. The line of drones from Axon and DJI is called the Axon Air, and the devices will be linked to Axon's cloud-based database for law enforcement, Evidence.com, which is used to process body-camera data too. And it could open a vast new frontier for police surveillance.

By working with a company that is already familiar with contracting with police departments, the Chinese-owned DJI—the world's biggest consumer drone manufacturer—could widen up a new, growing customer base: cops. Axon Air, which was announced Tuesday by Axon, is marketed as a way to help law enforcement with search-and-rescue operations, crowd monitoring, traffic-accident reconstruction, and evidence collection. It will make drone data the latest addition to Axon's suite of tools for police, which include tasers, body cameras (of which Axon is the country's biggest seller), and car cameras. Axon CEO Rick Smith recently said that his company is actively considering using facial recognition with its camera technology.

The company seems to be aware of the troubling societal implications—or at least the ugly optics—of such a move, announcing in April that it was setting up an artificial intelligence–ethics board to inform its use of A.I. in police surveillance tech. Nevertheless, that announcement sparked serious concerns, among civil rights and technology-privacy advocates including the NAACP and the American Civil Liberties Union, that pairing Axon's products with A.I. could further perpetuate racial profiling by police. For example, a mug-shot database that may be scanned to match footage from a police body camera is likely to have more photos of black faces than white ones. So if police pull over a black driver, the officer could be more likely to match his or her image with a mug shot and engage in further questioning, while a white person pulled over might be less likely to generate a match.

Despite Smith's statement, Axon told me it isn't currently working to deploy facial recognition in its cameras. "While we do see the value in this future capability, we also appreciate the concerns around privacy rights and the risks associated with mis-identification of individuals," spokesman Steve Tuttle wrote in an email. But it's not just surveillance that some advocates are wary of when it comes to the police-tech company getting into the drone game. "Axon also makes tasers, so you could imagine drones being equipped

with tasers or with tear gas, rubber bullets, and other weaponry," said Harlan Yu, the executive director of Upturn, a policy nonprofit that works on social justice and technology issues. This isn't necessarily hypothetical. In 2015, the North Dakota legislature passed a law that legalized the use of armed drones by law enforcement, Yu pointed out. Axon has already demonstrated how a stun gun can be added to a drone.

Evidence.com, according to Axon's press release, is currently used by more than 200,000 public-safety professionals. According to Axon's Tuttle, "all digital data including PDFs, crime scene photos, CCTV footage, in-car cameras, and now DJI drone video can be associated to a single case file"—meaning it's possible to look up a case involving a camera mounted in a police car and see if the same case also has drone footage associated with it. Tuttle said that law enforcement agencies own what they upload to Evidence.com, even though the repository itself is owned and maintained by the company. But that doesn't mean police departments can't share that data with other law enforcement agencies—many already share their surveillance data, through various databases—nor does it mean Axon can't request to access to the data to, say, train artificial intelligence systems. Vigilant Solutions, a police-surveillance-technology company that specializes in storing license-plate-reader data used by law enforcement, allows police departments and federal agencies across the country to share their data with each other, including at times between police departments in sanctuary cities and agencies within Immigration and Customs Enforcement.

By combining drone, body-camera, police-car-camera, and closed-circuit-TV footage, Axon is clearly hoping to create a central hub for police to cross-reference and access surveillance data—a treasure chest of information that, according to Elizabeth Joh, a law professor at the University of California–Davis who studies civil liberties and police surveillance technology, police departments could find difficult to stop using once they start. "Not only is there no real competition from other vendors," said Joh, "but once a police department has bought into a certain contract with a company, it's very hard to drop it and move on. There's a lot of investment in training the agency and the officers how to use it." Which could raise a competition issue, with Axon positioning itself as a panoptical must-subscribe for law enforcement agencies. "The question here is whether we want this kind of tech monopoly

at a time when it's clear that tech monopolies like Facebook haven't really served the public interest that well," said Joh.

The monopoly question with Axon isn't just about departments being locked into the company's service because of a lack of competition or switching costs. It's also about how the company could monetize its access to police data in the future. Axon's dominance in the police-camera surveillance-data market could give the company an unbeatable leg up. That's because the more data A.I. has to train itself on, the better it is, and so whatever company has the most data will likely have the best product. Axon did, after all, acquire two different artificial intelligence companies for analyzing video footage last year, which the company said in a press release will be combined to form a new division, Axon AI.

A DJI spokesperson said that its "partnership with Axon does not include any attachments with offensive capability, or any facial recognition technology"—but once a drone is purchased and in the hands of law enforcement, it's theirs to do what they want within the bounds of the law. That could mean surveilling a protest with a drone, which is something police have certainly explored doing in the past. In May, Chicago Mayor Rahm Emanuel threw his support behind a bill that would permit police to fly drones over large events for surveillance. And Amazon has been marketing its facial recognition software, Rekognition, which can identify up to 100 people in a single photo, to law enforcement agencies for the past two years. There's no reason to think that software couldn't be applied to drone footage, whether the capability is contained within the drone itself or is applied to footage sent to a computer on the ground in real time.

"There are good uses of drones that we don't object to in limited situations where it makes sense to have a camera in the sky, whether it's for construction or for finding a lost child in the woods," said Jay Stanley, senior policy analyst at the ACLU. He said he becomes concerned with the technology when it ends up being used to monitor a wide area, like by flying over a city broadly collecting data from the air. "It could give police the ability to hit rewind on people's lives and see anywhere they've been," he said.

It's not unusual for police departments to procure surveillance technologies without public discussion. But communities concerned about police use of surveillance drones aren't without recourse. Oakland, California, passed a

strong new ordinance regulating police use of surveillance technologies in May, requiring any surveillance technology that the city wants to be subject to review and approval by a local board of volunteer commissioners. In doing so, police must disclose and engage in conversation around new surveillance technologies they wish to deploy, meaning they couldn't buy surveillance drones without disclosing that information to the public. The California legislature is currently considering a statewide model for this kind of police surveillance privacy check.

"When municipalities are considering the adoption of drones, they need to be extremely careful," said Yu. "They need to consult with communities before adopting these technologies to get their approval, and whether its drones and other police technologies, it should be a democratic decision."