Wolfcom’s Facial Recognition Body Cameras

By Melissa Giddings

As facial recognition products proliferate, some companies are marketing increasingly invasive versions of the technology. Worryingly, surveillance technology manufacturer Wolfcom is proposing body cameras with a live facial recognition function to law enforcement agencies across the United States. In contrast to static uses of the technology, where police compare a photo to large databases of mugshots or licenses, “real-time” facial recognition involves the constant scanning of live video feeds to match moving faces with a database of still images. When we give law enforcement the extraordinary power to track people in real time, we erode our freedom to associate, speak, and live private lives.

A former Hollywood-based paintball retailer, Wolfcom started making body-worn cameras in 2011, moving to Pasadena and shutting down its paintball operations in 2015. In the ensuing years, Wolfcom has won about $100,000 in federal government contracts, mostly with the Department of Defense. The company has sold more than a million body-worn cameras to 1,500 agencies in more than 35 countries.

As reported by OneZero, Wolfcom sent an email to multiple police departments in May 2019 requesting they test a developing facial recognition software. Wolfcom founder Peter Austin Onruang wrote that by incorporating real-time facial recognition into its products, Wolfcom “hopes to give our friends in Law Enforcement tools that will help them identify if the person they are talking to is a wanted suspect, a missing child or adult, or a person of interest.”

Wolfcom markets three models of body-worn cameras to law enforcement. The addition of facial recognition to their newest model, the “Halo,” makes Wolfcom the first major body-worn camera provider in the U.S. to pursue live facial recognition. While all body-worn cameras can capture still photos and feed them into a facial recognition database, live facial recognition poses a unique danger, allowing police to collect identifying information without a person’s knowledge or consent.

In a video demonstration shared by the company, the Halo camera is paired with a facial recognition–enabled computer that automatically identifies the faces of three volunteers. As the volunteers enter the body-worn camera’s field of vision, the Halo’s facial recognition and computer vision software compares them to a database of known individuals, predicts certain demographic characteristics such as age and gender, and determines if they are subject to an outstanding warrant or are a missing person.

---

There are numerous unanswered questions about Wolfcom’s real-time facial recognition software. Facial recognition is frequently less accurate for women, especially women of color, which leads to increased misidentifications. Wolfcom has made no claims about accuracy and has not disclosed which databases it accesses to match faces. It is also unclear whether Wolfcom created the facial recognition software itself or is licensing it from a third party.

Law enforcement agencies have long argued that body-worn cameras will prevent police brutality and discrimination, but many questions remain about whether this proves true in practice. In 2015, U.S. Attorney General Loretta Lynch promised “transparency, accountability and credibility” when announcing a $23 million bodycam pilot program. This promise is far from the reality.

Already, lax departmental policies give officers discretion over when and what to record on their body cameras, and privacy protections focus more on protecting officers than the general public. Often, the tools that are sold as a mechanism to hold officers accountable are used to distort the public’s idea of police activity. And police departments frequently stonewall disclosure of unfavorable recordings. As one example, the New York Police Department failed to release bodycam footage in 40 percent of cases where it was requested by the Civilian Complaint Review Board. It doesn’t take much imagination to envision the possible abuse facial recognition–enabled body cameras could cause. Police departments could easily leverage the cameras to monitor people’s movements across the city, even absent outstanding warrants or suspected criminal activity.

Each officer-worn body camera captures information on every individual – suspect or not – that an officer encounters in a day. The privacy impact will only be amplified when facial recognition surveillance is integrated into the camera, allowing the police to turn a routine patrol into a warrantless search of where people go and with whom. An officer standing outside a church, addiction treatment center, political rally, or abortion clinic could chill our most fundamental constitutional rights.

Global demand for facial recognition technology means there are dozens of companies vying to contract with the government. NEC, a Japanese company which already sells static facial recognition technology to American jurisdictions, has sold real-time facial recognition elsewhere in the world, most recently to London’s police department.

But some major stakeholders and technology vendors recognize the risks posed by real-time facial recognition in body cameras. In October, California passed AB1215, barring police departments from using body cameras with live facial recognition software. Last year, Google announced it

---


would pause development of facial recognition products for governments. Axon, the country’s largest body camera supplier,9 announced it would ban live facial recognition on its products for the foreseeable future on the advice of its ethics advisory board,10 though the company has left open the possibility of adding the software to body-worn cameras in the future.

This has not dissuaded Wolfcom from developing its facial recognition–enabled Halo camera.11 Wolfcom has already started beta testing the product with Los Lunas Police Department in New Mexico,12 and the company’s website includes a password-protected download link for a facial recognition app for use on Android phones.13

Rather than rely on temporary pledges from technology companies to proceed ethically, lawmakers should impose regulations on the use of facial recognition technology. There are very few such regulations at the federal, state, or local level. Exceptions include Oregon and New Hampshire, which ban facial recognition on police-worn body cameras, and Maine and Vermont, which prohibit using such technology with police drones.14 The Surveillance Technology Oversight Project has consistently called for lawmakers in New York to catch up with these states in banning police use of facial recognition or any biometric surveillance system.15

We have the power to reject surveillance that is invasive, discriminatory, and far-reaching. Decisions about whether law enforcement should be able to identify you in the course of visiting friends, participating in protests, voting, attending church, or seeking medical care should not be made by tech companies or police departments.

---

12 See Gershgorn, supra note 1.