Doorbell Cameras Like Ring Give Early Warning of Police Searches, FBI Warned

Sam Biddle ⋮ 5-6 minutes ⋮ 8/31/2020

The rise of the internet-connected home security camera has generally been a boon to police, as owners of these devices can (and frequently do) share footage with cops at the touch of a button. But according to a leaked FBI bulletin, law enforcement has discovered an ironic downside to ubiquitous privatized surveillance: The cameras are alerting residents when police show up to conduct searches.

A November 2019 "technical analysis bulletin" from the FBI provides an overview of "opportunities and challenges" for police from networked security systems like Amazon's Ring and other "internet of things," or IoT, devices. Marked unclassified but "law enforcement sensitive" and for official use only, the document was included as part of the BlueLeaks cache of material hacked from the websites of fusion centers and other law enforcement entities.

The "opportunities" described are largely what you'd expect: Sensor-packed smart devices create vast volumes of data that can be combed through by curious investigators, particularly "valuable data regarding device owners' movements in real-time and on a historic basis, which can be used to, among other things, confirm or contradict subject alibis or statements."

The downside for police, who have rushed to embrace Ring usage nationwide as the Amazon subsidiary aggressively marketed itself to and sealed partnerships with local departments, is that networked cameras record cops just as easily as the rest of us. Ring's cameras are so popular in part because of how the company markets their ability to detect motion at your doorstep, providing convenient phone alerts of "suspicious activity," however you might define it, even when you're out of the house. But sometimes the police are the unannounced, unwanted visitor: "Subjects likely use IoT devices to hinder LE [law enforcement] investigations and possibly monitor LE activity," the bulletin states. "If used during the execution of a search, potential subjects could learn of LE's presence nearby, and LE personnel could have their images captured, thereby presenting a risk to their present and future safety."

> Law enforcement "personnel could have their images captured, thereby presenting a risk to their present and future safety."

The document describes a 2017 incident in which FBI agents approached a New Orleans home to serve a search warrant and were caught on video. "Through the Wi-Fi doorbell system, the subject of the warrant remotely viewed the activity at his residence from another location and contacted his neighbor and landlord regarding the FBI's presence there," it states.

This bulletin cites another unclassified but "law enforcement sensitive" FBI document about the same incident, titled "Video Doorbell Devices Pose Risk to Law Enforcement in New

Orleans, Louisiana as of 25 July 2017," which notes that a "subject was able to see and hear everything happening at his residence" and possibly "covertly monitor law enforcement activity while law enforcement was on the premises" via an unnamed make of "video doorbell." Such devices are sold under Amazon's Ring brand, Google's Nest, and by a variety of other companies.

The incident speaks to the unintended consequences of turning networked surveillance into just another consumer gadget. Internet-connected cameras are now just part of a growing array of always-scanning domestic sensors that accumulate great plumes of potentially incriminating private data on their owners (and potentially others in the vicinity), making obvious fodder for police surveillance efforts. They are also, clearly, a net negative to the privacy of those who have to live near them; the implications of the devices for sidewalk anonymity, overpolicing, and Fourth Amendment rights have been reported on and argued in great detail.

Tellingly, the bureau in its documents does not discuss that literally anyone who happens to walk within range of such a device, not just "LE personnel," could "have their images captured, thereby presenting a risk to their present and future safety." But the bulletins illustrate that it's at least possible for the American public/private security apparatus to sometimes backfire in the form of this sort of reverse surveillance, turning smart lenses into an obstacle for police instead of an obedient asset. Still, this phenomenon, and its potential as a countervailing force for civil libertarians, could remain very much an edge case. If the balance of power in public/private law enforcement schemes typified by Ring (and its corporate parent, Amazon) remain tipped in favor of the police, it may be because that's just who the system was designed to help — and because of the simple fact that most people walking past a Ring camera's never-blinking lens simply aren't going to be cops in the first place. It stands to reason that a company that's made "Fuck Crime" an internal motto and "dirtbag criminals" an avowed enemy is unlikely to savor the possibility that its products could save their customers from FBI scrutiny.