getpocket.com

The Doorbells Have Eyes: The Privacy Battle Brewing Over Home Security Cameras

Geoffrey A. Fowler

9-12 minutes

Doorbells are gaining cameras for security and catching porch pirates. The Post's Geoff Fowler goes over security camera etiquette you may not have considered. (Jhaan Elker, Geoffrey Fowler/The Washington Post)

Ding-dong, your doorbell is looking a bit creepy.

Ring video doorbells, Nest Hello and other connected security cameras are the fastest-growing home improvement gadgets since garage-door openers. These cameras, often built into buzzers, alert your phone when someone is at your door and save footage online. Mine has helped me get deliveries and catch porch pirates stealing

packages. In January 2019, one caught a man licking a family's doorbell for three hours.

What's not to love? Invading people's privacy — and Big Brother at our doorstep. It's up to us to set the rules to avoid Big Doorbell.

We're on a slippery slope. You've got a legal right to film in public places, including your entryway. There's little agreement whether private cameras slash crime rates, yet police are setting up voluntary registries for private cameras in dozens of communities. Cities such as Washington have begun paying up to $500 for cameras on private property. Detroit is going further: Its mayor wants to mandate security cameras at businesses open late, with a live feed going straight to police.

Meanwhile, Ring's owner Amazon.com filed an eerily specific patent to put its controversial Rekognition facial-identification software into doorbells. The purpose: to automatically flag "suspicious" people. (Amazon CEO Jeffrey P. Bezos owns The Washington Post, but I review all tech with the same critical eye.)

We should recognize this pattern: Tech that seems

like an obvious good can develop darker dimensions as capabilities improve and data shifts into new hands. A terms-of-service update, a face-recognition upgrade or a hack could turn your doorbell into a privacy invasion you didn't see coming.

In early 2019, Ring got caught allowing its team in Ukraine to view and annotate certain user videos; the company says it only looks at publicly shared videos and those from Ring owners who provide consent. Not long after, a California family's Nest camera let a hacker take over and broadcast fake audio warnings about a missile attack, not to mention peer in on them, when they used a weak password.

In the future, what if your doorbell misidentified someone as a crime suspect? What if it logs a "dreamer" — an undocumented immigrant brought to the United States as a child — visiting, or living in, your house? Your family and friends are the ones whom this tech surveils the most.

Okay, Big Doorbell hasn't yet evolved to the point where police are peering through live to see who's coming over for dinner. But we probably don't want

to build that.

How do we stop a potential civil liberties nightmare? By talking about ethics now.

I'm worried the giant tech companies, who don't have a stellar record of protecting us, aren't being very specific about getting the balance right. Ring says that facial recognition patent "certainly does not imply implementation," but it also wouldn't draw lines in the sand about what it won't do with the face tech. Nor would Nest, owned by Google.

Both companies say they care about privacy, but neither company's senior executives would discuss their ethical lines with me.

They won't, but we can. We can already identify lines these technologies probably shouldn't cross. So I spoke to lawyers, city officials and criminologists to make an ethical field guide for people who want tech to help us stay safe — but don't want to be creeps.

---

1. Don't point your camera at neighbors.

An original premise of Ring, which inventor Jamie Siminoff pitched on "Shark Tank," was that a camera

in a doorbell makes privacy sense. The entryway is where someone presents themselves for inspection.

Over time, though, the cameras have captured a lot more than people pressing doorbells. With new models built into more places — outdoor floodlights, garage doors, even peepholes — they're also recording the street and maybe the neighbors, too.

Focus your camera on your own castle only. Keeping a digital record of every time a neighbor comes home is basically stalker behavior. If your doorbell is located in an awkward place, you can try to use wedges to angle the camera toward your door. Some cameras let you mark zones to limit recording only to action that's important for your home.

Also: Let people know they're on camera. Put up a sign to flag you're filming — it might also deter a potential burglar.

---

2. Share footage sparingly.

But hold on, Columbo: Are you actually an expert in what counts as "suspicious"? Sharing on these sites can help fight crime but can also perpetuate racial

profiling. (Ring says it proactively moderates content uploaded to its app to ensure it is in accordance with its community guidelines.) Focus on evidence of actual crimes.

---

3. When police get involved, it should be voluntary.

Most people are happy to help police catch criminals. But when and how should the police get access to your footage? The lesson from Washington: Make it voluntary.

The District of Columbia pays a rebate on up to two cameras at a home or business, in exchange for signing up on a police registry. Michelle Garcia, who runs the program that has paid for more than 10,000 cameras, says “law enforcement doesn’t have a right to the footage” — at least without a court order. She says she has not encountered cases where people won’t share, and that usually people seek out the police with footage.

Civil liberties advocates are still concerned people could feel compelled to share because they got a rebate or are in a registry. “When you eliminate the

friction between government and people that has traditionally existed, it can put people in situations where you take away their control over privacy," says Matt Cagle, a lawyer at the American Civil Liberties Union of Northern California.

Ensuring that private footage remains private is one important way to keep us from a police state. A Ring spokeswoman says: "Our customers are in control of who views their footage. Period. We do not have any plans to change this." But would Ring draw an ethical line at sharing footage directly with police, even if there was consent? It wouldn't say.

A Nest spokeswoman gave a firmer "no" to whether it would ever share footage directly with police.

---

4. Delete old footage.

Cagle has some practical advice for camera owners: Just delete. It's hard to understand today how footage might be used — or abused — tomorrow. "The more you have, the more vulnerable you are," Cagle told me.

But might you need old footage? You'll probably know if a crime happened at your house that day.

Even the D.C. program only asks participants to hold on to old footage for 48 hours. Unfortunately, Ring and Nest don't make it easy to comply: Ring's basic plans hold on to footage for two months, and Nest's plan starts with five days.

---

5. Keeping hackers out is a serious responsibility.

If someone hacks into your security camera, you could expose all the people who have passed by your camera — including friends, family and yourself. Some of the responsibility is with the makers of these cameras to keep their systems secure. But we have to do our part, too, by updating software, using unique passwords and taking other security protections. If you aren't sure you know how to do that, don't buy one of these devices.

That California family who got the creepy audio warnings about a missile attack messed up by using a not-very-secure password. (See my suggestions on how to do better by using a password manager.) They also failed to turn on an additional protection from Nest called two-factor authentication, which

would have alerted them about unauthorized access with a text message. Ring still doesn't offer two-factor authentication.

---

6. Facial recognition isn't a product feature: It's a superpower.

Who doesn't want to be safe? That's how tech companies market most of these products. But there's one coming feature where we should challenge that thinking: facial recognition.

The ability to keep tabs on a person's whereabouts by reading their face is a superpower we don't yet have the legal or ethical framework to handle. As the tech improves, it'll be a slow march toward omniscience. First, our cameras will offer to flag family members' faces — Nest already offers that in its camera. Next, they'll link to a few public databases: a terrorist watch list, missing children, sexual offenders. But who gets to make those lists, and how accurate are the systems flagging people?

That Amazon patent for Rekognition in doorbells spooked civil liberties advocates. The company says it was just an idea. "To ensure our technologies

benefit customers, we take the time to carefully consider how each new feature or product will add value for our users, how they will use it, and whether it's in line with our three pillars of privacy, security and consent," a spokeswoman said in a statement. But would it draw a line at connecting to public face databases? Ring wouldn't say.

Nest says its "familiar faces" service limits the library of faces to one family and is "not shared across users or used in other homes." That's for now, at least — Nest had no answer about future use.

With great power comes great responsibility.