Facial recognition technology: In our rush to deploy it, are we ignoring the risks?

February 13 2020, by Khalida Sarwari

Nearly 400,000 Ring doorbells were sold in December, making it the biggest month for sales ever—in the same month that the company came under fire for multiple hacks. Northeastern professor David Choffnes surmises that convenience and fear were likely driving these sales. Credit: Matthew Modoono/Northeastern University

Taylor Swift uses it to identify stalkers. Retail stores are using it to provide a no-checkout, cashierless experience. Even churches are getting in on it to keep track of their congregants.

Increasingly, facial recognition software—technology that readily identifies people based on their faces—has found its way into the most intimate corners of our lives.

The benefits, we're told, are myriad. Law enforcement agencies, airports, and business owners have been quick to adopt the tool in the name of safety and security. And, retailers and social media platforms tout convenience as a big reason for why they have jumped on the facial recognition bandwagon.

Last month, London's police department announced that it would begin installing cameras in locations popular with shoppers and tourists to spot criminal suspects, making London the latest in a growing list of cities that have embraced facial recognition. The decision has stirred an ongoing debate among privacy advocates about how to properly balance security with individual privacy and liberty.

David Choffnes, an associate professor at Northeastern whose research focuses on distributed systems, networking, privacy, and security, cautions that with so much at stake, it's worth considering the potential risks of these surveillance tools before rushing to deploy them.

"I think that we need to really understand the risks of these technologies before we deploy them at a very large scale, where unknown risks could manifest at extremely large scale," says Choffnes, who is a founding member of Northeastern's Cybersecurity and Privacy Institute.

The benefits from a public safety perspective are fairly easy to understand, he says. If someone steals a car or kidnaps a child, video

surveillance can make the difference between identifying the perpetrator within hours of the crime occurring, when law enforcement officers have the highest chance of solving a crime. It was an ad hoc surveillance network, after all, that helped authorities quickly identify and find the suspects in the 2013 Boston Marathon bombing.

"A big motivator for the deployments that we see today is crime," says Choffnes. "[The thinking goes] there are cases that may have been solved if we had surveillance footage at the place where the criminals were, so let's put it up everywhere."

On the other hand, he says, we mustn't overlook the existing cases of abuse, misuse, and unauthorized use of surveillance data. This has enabled all kinds of malicious behavior, including stalking, blackmail, and casing locations.

"The bottom line is that the more surveillance there is, the more opportunity there is for that data to be compromised or abused," Choffnes says. "And if the data wasn't there in the first place, there would be no opportunity for that."

At this point, it's difficult to know all the harms and benefits of facial recognition or public surveillance cameras, says Choffnes. He has grave concerns over how certain governments have used facial recognition to track and arrest peaceful, pro-democracy demonstrators.

"That's the kind of thing that I worry about longer term is how this could be used against law-abiding citizens," he says. "And ultimately, we don't have the data to know or quantify what are the benefits and whether or not the harms outweigh those benefits."

As part of a research project last year, Choffnes found that Ring devices, which are wireless video doorbells for people to see visitors at

their doorstep, used motion sensors to record visitors for 10 seconds with no indication to those visitors that they were being filmed.

The company, which is owned by Amazon, has received criticism for partnering with more than 400 police departments. Ring has said that the partnerships were formed to assist in police investigations, and provide additional protection against criminals and intruders.

Then, last month, it was revealed that the device's mobile application is packed with third-party trackers that send out personal information to analytics and marketing companies, including the customer's name, IP address, mobile network carrier, and sensor data. Choffnes isn't surprised by the news.

"I think that when some consumers learn that video data is being shared, they will say great, send it to law enforcement [and other parties]; I have nothing to hide," he says. "And others might realize that they don't want to have a feed of activities around their home, including their own activities, sent to police and archived indefinitely, especially without their knowledge and informed consent."

And yet, online sales of the device have skyrocketed. Nearly 400,000 Ring doorbells were sold in December, making it the biggest month for sales ever—in the same month that the company came under fire for multiple hacks. Choffnes surmises that convenience and fear were likely driving these sales.

"There is also a reinforcing effect," he says. "If you see your neighbor posting images of someone stealing something from their doorstep, then you think, "Hey, that's a cool device that allows them to know what happened, now I want one, too, because it makes me feel more secure if I have this device." Of course, the irony is that it doesn't actually provide additional protection against someone stealing packages."

Choffnes says he does not own a Ring—or any other—video doorbell.

"I've learned enough from Internet-connected doorbells to keep them safely confined to my lab," he says.

Provided by Northeastern University