Pittsburgh researchers can’t stop tech giants or hackers from using your data. But they can try to protect your identity

LAUREN ROSENBLATT
Pittsburgh Post-Gazette

AUG 14, 2021 | 9:14 PM

One in an occasional series

During a pandemic that required us to stay far away from one another and cover up most of our faces with a mask, one health and safety measure has led us to get up close and personal — with our own face.

To help prevent the spread of COVID-19, many public buildings and event spaces set up temperature scanners. Some look like a radar gun while others are more intimate, complete with a front-facing camera that highlights every hair that’s out of place. While they’re checking for a fever, a little bit of your privacy is being taken, too, tracking your movements, your schedule and even your hairstyle changes.

Does it matter?

Questions about the future of the multi-billion smart technology industry that tracks what we are doing are more than theoretical in Pittsburgh. Researchers at places like Carnegie Mellon University are studying the implications of all this data collection and working to find alternate ways to tap into the benefits without sacrificing each user's personal information.

"We should assume we live in a society where all this information can get out there," said Chris Harrison, a researcher and professor at Carnegie Mellon University's Human-Computer Interaction Institute.

In February, NPD Group reported half of U.S. homes have at least one smart home device. And it would be hard to find a smartphone without at least one app installed that tracks movement and location. Do we want the cool new tech? Or do we worry about protecting our privacy? These researchers say we want both.

The public health crisis of the COVID-19 pandemic provides a case in point. It tipped the scales in favor of loosening protections — think apps that track vaccination status or contact tracing efforts — to benefit the public good. What happens when the public health crisis abates?

Chris Harrison, left, associate professor of Human-Computer Interaction at the Carnegie Mellon University and Karan Ahuja, a Ph.D. student in Human-Computer Interaction at CMU, working on a way to use Doppler radar to track movements.
(Pittsburgh Post-Gazette)

"There's a general tendency — but not true for everyone — for people to be more accepting of data collection processes in return for that sense of safety and security," said Norman Sadeh, a computer science professor at CMU

who studies privacy related to the Internet of Things, or the network of sensors and other devices that are creating connected technologies like smart toasters and refrigerators.

“COVID was just an example of yet another reason for us to potentially try to collect more data,” he said.

“When it’s done for health reasons and public safety reasons, there are exceptions and by and large we are expected to give up some level of privacy. But very quickly, this data starts being used for other purposes.”

Late night espionage

Picture this: You go downstairs to get a midnight snack in your pajamas.

You think you’ve made it through unnoticed — no family members woke up and that missing slice of cake is barely noticeable — until you open the TikTok app on your phone the next morning.

There you are: pajamas, cake and all.

If you have a sensing device like an Alexa or Google Home that keeps a camera trained on the kitchen to remind you to wipe down the counters, that device is also collecting less pertinent images and information.

In reality, it’s not likely someone would hack into a smart home device just to steal raw footage of your late-night snacking. But the presence of these types of technologies is enough to raise concerns.

One solution? Make sure potential data leaks aren’t damaging.

Karan Ahuja, a Ph.D. student in Human-Computer Interaction at CMU, solder components together that will be used to track movement Thursday, July 15, 2021, at Carnegie Mellon University in Oakland.
(Pittsburgh Post-Gazette)

Mr. Harrison and his team at CMU are working on an alternative to sensing devices that rely on cameras and visual cues. Instead, the system uses Doppler radar to collect information about user's locations and movements in a room.

It is trained to recognize 12 activities — from cleaning to clapping to different types of exercise — without giving away the identity of the person performing those actions.

Dong Huang, a researcher from CMU's Robotics Institute, is working on the same problem with a different method. His team's sensing system uses WiFi signals from routers already set up in most people's homes.

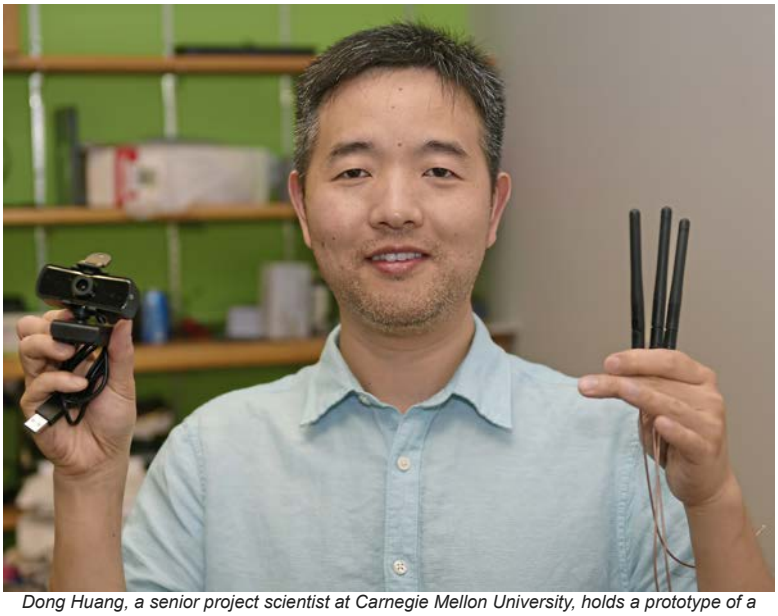
This system looks at how the signals reflect off the furniture, walls and humans and then uses deep learning to make predictions about the bodies in the room and their poses and movements.

The Doppler radar system is still in the research phase, Mr. Harrison said, while Mr. Huang's team hopes to have a prototype of its WiFi sensing system by the end of the summer.

A debate that started with Kodak

COVID-19 may have been a catalyst but concerns over what information was being collected and for what purpose started long before Bluetooth, WiFi, iPhones and consumer versions of sensing technologies even existed.

Alessandro Acquisti, a professor of information technology and public policy at the Heinz College at CMU, dates it back to the invention of Kodak cameras.



Dong Huang, a senior project scientist at Carnegie Mellon University, holds a prototype of a device he and his team are developing that uses WiFi to track movements.
(Pittsburgh Post-Gazette)

Suddenly, it was easy to snap pictures at a wedding and run them in the newspaper. Every private space had the chance to go public.

He cited a paper from the 1890s that warned the personal cameras were a threat to privacy. Those same arguments still apply, Mr. Acquisti said. Just replace Kodak with Instagram.

He has a theory that there have been three turning points in the latest conversations around tech and privacy. 1. The internet. 2. Social media apps like Facebook. 3. Cell phones.

“We started becoming more and more accustomed to carrying remarkably powerful surveillance devices in our pockets at all times,” he said. “Which is

why I don't believe the pandemic has truly altered our conceptions of privacy or our comfort with being tracked.

"This is a process that started way back."

Automated cameras in the home raise a new level of concern.

"With respect to devices, having a teleconference with your doctor is one thing," Mr. Harrison said. "Having Amazon, Google, Facebook with a camera on it is something entirely different. To have an artificial intelligence application in your home that has a camera on it raises this specter of privacy invasion beyond what most consumers want."

A hard problem to tackle

When it comes to protecting the data collected from mobile phones and social media sites, it can feel out of the user's control. The same goes for tech entrepreneurs looking at how to bake privacy into their new products.

"Increasingly, our data is controlled by fewer and fewer mega-corporations," said Jim Wrubel, a portfolio executive at North Shore-based startup investor Innovation Works. "I can't start a company to help you prevent Facebook from stealing your data. Because it's up to them to decide what they do and don't do."

Recently, lawmakers and even some tech companies have started to get involved in that decision.

Federally, legislators have discussed data privacy laws and cracking down on antitrust cases. In California, the Consumer Privacy Act codifies the right to know what personal information a business collects and how it is used and shared. It also allows users to opt out of the sale of their information and the right to delete some of that data.

In April, Apple rolled out an update that required apps to get the user's permission before tracking their data across other apps or websites owned by different companies.

At CMU, Mr. Sadeh and his team developed an algorithm to make it easier for users to understand what data collection they are agreeing to before it happens.

The group created a web browser extension that uses machine learning to quickly read through those lengthy terms and conditions that users are

expected to agree to before moving forward on a website or app. The algorithm will pull out the important parts so people can figure out what exactly they are signing up for.

“Privacy is a secondary task,” Mr. Sadeh said, so his team wants to make it more efficient.

Sensing control

Mr. Harrison, the CMU researcher creating sensing tech that relies on Doppler radar, sees his team’s role as putting “the right tools into the public imagination.” The goal is to spark interest in “non-camera approaches” to delivering the same types of services as smart home devices.

Think about a research project to develop technology that alerts people when a package has been delivered. Most people’s first thought is to put a microphone on the door to pick up the sound of the bell, Mr. Harrison said. But, what if there was a way to recognize the doorbell without picking up the gossip you spread with your neighbor before heading inside?

He suggested a doorbell that also sends a chirp, like a radio signal, and a device to pick up that sound, rather than all outside noise.

Mr. Huang, who is developing the WiFi system at CMU, pictures this type of tech being used to augment home security systems or health care for seniors. Because it collects data “just for what we need,” it can keep an eye on whether someone falls when getting out of bed — without keeping a record of what they wore to bed.

Shipments of smart home devices — from home security systems to smart speakers — reached 801 million units globally in 2020, according to a March report from the International Data Corporation, a market intelligence firm based in Massachusetts. By 2025, sales are projected to break 1.4 billion.

The researchers say there’s a market for tech that offers the benefits of sensing devices without the privacy concerns.

But there are also hurdles to developing those systems: The WiFi system has trouble recognizing rare poses or small limbs. The Doppler radar system can’t yet “see” around corners. Mr. Harrison’s group also had to create a new way to train its artificial intelligence system since it couldn’t

rely on the massive library of videos and images that teach a device that collects visual cues.

A man checks his phone while walking through Steel Plaza Station, Downtown, on Tuesday, Aug. 3, 2021.
(Steve Mellon/Post-Gazette)

Sensing on the job

At Yodel Labs, a North Oakland-based company that spun out of CMU in 2017, researchers are working to bring tracking technology out of the home.

“These systems essentially act like GPS but for inside buildings,” said Patrick Lazik, co-founder and chief technology officer. “You pull out your phone in a big, complex building like an airport, hospital or convention center [and] the phone is able to localize very accurately … where you are in 3D space.”

Indoor localization tech could help users track down the cereal aisle in the grocery store or their gate at the airport.

The COVID-19 pandemic disrupted some of those indoor plans, Mr. Lazik said, so the company pivoted to the work site. It created a device that looks like and works in a similar way to an ID card, except it also keeps a record of other tags that worker was next to and for how long.

When it comes to worker safety amid a pandemic, that data can be used for contact tracing and to simulate the spread of a virus through the workplace, Mr. Lazik said.

He couldn't disclose who the company works with but did say some clients had privacy concerns. "Of course, people are hesitant with those kinds of things that track their location and every motion that they make," Mr. Lazik said. "That's not the case with our system. It only tracks who you've been in close contact with."

The company also set up safeguards to protect who can see the data and how far the location tracking goes. The work sites are outfitted with bay stations at entry and exit points and the data collected from the tag isn't available until the end of a shift, after the worker passes through the exit point and heads home for the day.

Just as researchers are predicting convenience may trump privacy when it comes to smart home devices, Yodel Labs predicts the public health benefit will outweigh concerns.

It's happened before.

"Time and time again — postal systems in the 1800s, telephones in the 1900s, video conferencing in the 2000s," Mr. Harrison said. "Every single time, we've taken convenience over privacy."

Lauren Rosenblatt: lrosenblatt@post-gazette.com, 412-263-1565.

First Published August 14, 2021, 7:07pm