YOUR APPLIANCES ARE KILLING YOUR FAMILY PRIVACY WITH HELP FROM GOOGLE AND FACEBOOK

Thu, 07 Sep 2023 09:52:03, swmof88, [category: news, post_tag: your-appliances-are-killing-your-family-privacy]

How doorbells, smart speakers, TVs and washing machines are spying on you: Research reveals how household appliances are capturing and sharing private data with firms such as Google, Amazon, Facebook and TikTok

Research shows that standard household amenities are capturing and sharing private information with big tech firms such as Google, as well as Amazon, Facebook and TikTok.

The household appliances spying on YOU: How doorbells, smart speakers, TVs and washing machines capture and share private data with firms such as Google and TikTok - so which are worst offenders?

- **Household amenities are sharing private info with big tech firms such as Google**

By SEAN POULTER CONSUMER AFFAIRS EDITOR

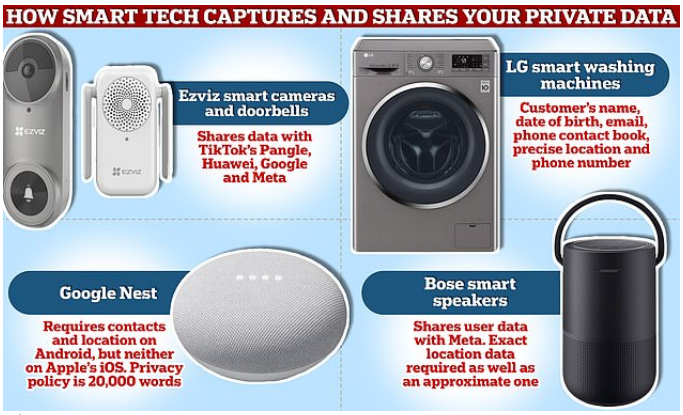
Everyday devices like smart speakers, doorbell cameras, TVs and even washing machines are spying on families, it has been revealed.

Research shows that standard household amenities are capturing and sharing private information with big tech firms such as Google, as well as Amazon, Facebook and TikTok.

It is believed the firms and their business partners are using the information to target people with advertising on smartphones and other devices.

The findings by Which? found companies appear to gather far more data than is needed for the product to function.

Google Nest smart home products, which include security cameras, smart speakers, doorbell cameras, heating control systems, gather a huge amount of location information on people who connect via smartphones using its Android operating system.



+4

View gallery

Your employer is watching you! Almost all major businesses now use monitoring software to track workers' keystrokes and web searches - with JP Morgan even checking time spent writing emails when they are IN the office

In a survey of some 1,000 businesses, ResumeBuilder.com found 96 percent were working at firms with either a remote or hybrid model said their firms used some form of monitoring software.

By contrast, these same Nest products gather much less information when the users connect to them via Apple's iPhones.

+4

View gallery

Which? said: 'It is not known why this additional data is collected. However, Google's primary business is advertising and marketing, whereas Apple currently focuses on selling hardware.'

Experts looked at what information the devices require to set up an account, what data permissions their apps request and what activity marketing companies are tracking on people's products.

Smart speakers are only supposed to listen when you want them to, but this is not always the extent of data collection.

For example, Bose smart speakers share user data with Meta, the parent company of Facebook.

Ezviz smart cameras and doorbells, which are sold by major retailers including Argos, had by far the most active tracking software.

This included sharing information with TikTok's business marketing unit, as well as Pangle, which is a leading video advertising platform, Huawei, Google and Meta.

+4

View gallery

Research shows that standard household amenities are capturing and sharing private information with big tech firms such as Google, as well as Amazon, Facebook and TikTok (File image)

Every single smart camera and doorbell brand used tracking services from Google, while Blink and Ring also connected to parent company Amazon.

Which? said the spy and tracking functions are automatically activated by default. Consumers can opt out, but this requires changing the settings and could lead to aspects of the device or app no longer working.

READ MORE: **The new neighbour rows being waged over Ring doorbells: Smart devices behind troubling rise in feuds after highly sensitive cameras pick up snippets of private conversations from as far as 40ft away**

Most smart TV menus are flooded with adverts, some personalised based on user data. While tracking is optional, Which? found that LG, Samsung and Sony bundle this up into an 'accept all' button.

LG wanted the most data of all the washing machine brands, including the customer's name, date of birth, email, phone contact book, precise location and phone number.

Hoover wanted users' contacts and phone numbers on Android devices. With Miele, tracking of precise location is enabled by default, and required to use its app.

A Which? survey found the data people were most concerned about being shared were their contacts and background location. This was followed by photos, phone number and precise location.

Under the General Data Protection Regulations (GDPR), companies must be transparent about the data they collect and how it is processed. The data collected must also be relevant and limited to what is necessary for the processing to take place.

However, the reasons for taking information are often too broad for consumers to appreciate, with companies claiming 'legitimate interests'.

+4

View gallery

- ## Google heads to court today to face Justice Department and group of states that accuse company of antitrust violations

Set to take place over the next 10 weeks, the proceedings will begin with both sides' opening argument in at 9:30am - with the Justice Department being the other principle.

It is believed the firms and their business partners are using the information to target people with advertising on smartphones and other devices (File image)

Which? policy director Rocio Concha said: 'Firms should not collect more data than they need to provide the service that's on offer, particularly if they are going to bury this important information in lengthy terms and conditions.

'The Information Commissioner's Office should consider updating guidelines to better protect consumers from accidentally giving up huge swathes of their own data without realising.'

Manufacturers argued they are transparent with customers about the use of their data. They argued that the data collected is used to improve devices and services.

Google said: 'Google fully complies with applicable privacy laws and provides transparency to our users regarding the data we collect and how we use it.'

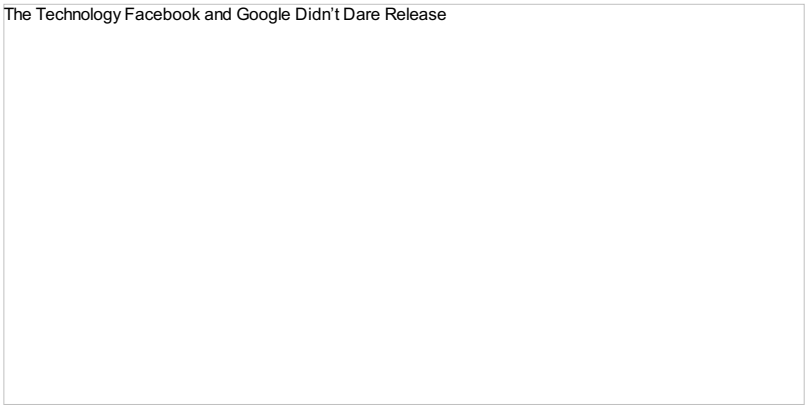
Amazon said: 'We design our products to protect our customers' privacy and security and to put our customers in control of their experience.

'We never sell their personal data, and we never stop working to keep their information safe. We use data responsibly to deliver what our customers expect: products that they love and are always getting better.' Other firms contacted by Which? did not respond.

Share or comment on this article: The household appliances spying on YOU: How doorbells, smart speakers, TVs and washing machines capture and share private data with firms such as Google and TikTok - so which are worst offenders?

The Technology Facebook and Google Use In Secret

The Technology Facebook and Google Didn't Dare Release



One afternoon in early 2017, at Facebook's headquarters in Menlo Park, Calif., an engineer named Tommer Leyvand sat in a conference room with a smartphone standing on the brim of his baseball cap. Rubber bands helped anchor it in place with the camera facing out. The absurd hat-phone, a particularly uncool version of the future, contained a secret tool known only to a small group of employees. What it could do was remarkable.

The handful of men in the room were laughing and speaking over one another in excitement, as captured in a video taken that day, until one of them asked for quiet. The room went silent; the demo was underway.

Mr. Leyvand turned toward a man across the table from him. The smartphone's camera lens — round, black, unblinking — hovered above Mr. Leyvand's forehead like a Cyclops eye as it took in the face before it. Two seconds later, a robotic female voice declared, "Zach Howard."

"That's me," confirmed Mr. Howard, a mechanical engineer.

An employee who saw the tech demonstration thought it was supposed to be a joke. But when the phone started correctly calling out names, he found it creepy, like something out of a dystopian movie.

The person-identifying hat-phone would be a godsend for someone with vision problems or face blindness, but it was risky. Facebook's previous deployment of facial recognition technology, to help people tag friends in photos, had caused an outcry from privacy advocates and led to a class-action lawsuit in Illinois in 2015 that ultimately cost the company $650 million.

With technology like that on Mr. Leyvand's head, Facebook could prevent users from ever forgetting a colleague's name, give a reminder at a cocktail party that an acquaintance had kids to ask about or help find someone at a crowded conference. However, six years later, the company now known as Meta has not released a version of that product and Mr. Leyvand has departed for Apple to work on its Vision Pro augmented reality glasses.

In recent years, the start-ups Clearview AI and PimEyes have pushed the boundaries of what the public thought was possible by releasing face search engines paired with millions of photos from the public web (PimEyes) or even billions (Clearview). With these tools, available to the police in the case of Clearview AI and the public at large in the case of PimEyes, a snapshot of someone can be used to find other online photos where that face appears, potentially revealing a name, social media profiles or information a person would never want to be linked to publicly, such as risqué photos.

What these start-ups had done wasn't a technological breakthrough; it was an ethical one. Tech giants had developed the ability to recognize unknown people's faces years earlier, but had chosen to hold the technology back, deciding that the most extreme version — putting a name to a stranger's face — was too dangerous to make widely available.

Now that the taboo has been broken, facial recognition technology could become ubiquitous. Currently used by the police to solve crimes, authoritarian governments to monitor their citizens and businesses to keep out their enemies, it may soon be a tool in all our hands, an app on our phone — or in augmented reality glasses — that would usher in a world with no strangers.

'We decided to stop'

As early as 2011, a Google engineer revealed he had been working on a tool to Google someone's face and bring up other online photos of them. Months later, Google's chairman, Eric Schmidt, said in an onstage interview that Google "built that technology, and we withheld it."

"As far as I know, it's the only technology that Google built and, after looking at it, we decided to stop," Mr. Schmidt said.

Advertently or not, the tech giants also helped hold the technology back from general circulation by snapping up the most advanced start-ups that offered it. In 2010, Apple bought a promising Swedish facial recognition company called Polar Rose. In 2011, Google acquired a U.S. face recognition company popular with federal agencies called PittPatt. And in 2012, Facebook purchased the Israeli company Face.com. In each case, the new owners shut down the acquired companies' services to outsiders. The Silicon Valley heavyweights were the de facto gatekeepers for how and whether the tech would be used.

Facebook, Google and Apple deployed facial recognition technology in what they considered to be relatively benign ways: as a security tool to unlock a smartphone, a more efficient way to tag known friends in photos and an organizational tool to categorize smartphone photos by the faces of the people in them.

In the last few years, though, the gates have been trampled by smaller, more aggressive companies, such as Clearview AI and PimEyes. What allowed the shift was the open-source nature of neural network technology, which now underpins most artificial intelligence software.

Understanding the path of facial recognition technology will help us navigate what is to come with other advancements in A.I., such as image- and text-generation tools. The power to decide what they can and can't do will increasingly be determined by anyone with a bit of tech savvy, who may not pay heed to what the general public considers acceptable.

‘Standing on the shoulders of giants’

How did we get to this point where someone can spot a “hot dad” on a Manhattan sidewalk and then use PimEyes to try to find out who he is and where he works? The short answer is a combination of free code shared online, a vast array of public photos, academic papers explaining how to put it all together and a cavalier attitude toward laws governing privacy.

The Clearview AI co-founder Hoan Ton-That, who led his company’s technological development, had no special background in biometrics. Before Clearview AI, he made Facebook quizzes, iPhone games and silly apps, such as “Trump Hair” to make a person in a photo appear to be coifed like the former president.

In his quest to create a groundbreaking and more lucrative app, Mr. Ton-That turned to free online resources, such as OpenFace — a “face recognition library” created by a group at Carnegie Mellon University. The code library was available on GitHub, with a warning: “Please use responsibly!”

“We do not support the use of this project in applications that violate privacy and security,” read the statement. “We are using this to help cognitively impaired users sense and understand the world around them.”

It was a noble request but completely unenforceable.

Mr. Ton-That got the OpenFace code up and running, but it wasn’t perfect, so he kept searching, wandering through the academic literature and code repositories, trying out this and that to see what worked. He was like a person walking through an orchard, sampling the fruit of decades of research, ripe for the picking and gloriously free.

“I couldn’t have done it if I had to build it from scratch,” he said, name-dropping some of the researchers who had advanced computer vision and artificial intelligence, including Geoffrey Hinton, “the godfather of A.I.” “I was standing on the shoulders of giants.”

Mr. Ton-That is still building. Clearview has developed a version of its app that works with augmented reality glasses, a more fully formed realization of the face-calling hat that the Facebook engineering team had rigged up years earlier.

The end of anonymity

The $999 pair of augmented reality glasses, made by a company called Vuzix, connects the wearer to Clearview’s database of 30 billion faces. Clearview’s A.R. app, which can identity someone up to 10 feet away, is not yet publicly available, but the Air Force has provided funding for its possible use at military bases.

On a fall afternoon, Mr. Ton-That demonstrated the glasses for me at his spokeswoman’s apartment on the Upper West Side of Manhattan, putting them on and looking toward me.

“Ooooh, 176 photos,” he said. “Aspen Ideas Festival. Kashmir Hill,” he read from the image caption on one of the photos that came up.

Then he handed the glasses to me. I put them on. Though they looked clunky, they were lightweight and fit naturally. Mr. Ton-That said he had tried out other augmented reality glasses, but these had performed best. “They’ve got a new version coming,” he said. “And they’ll look cooler, more hipster.”

When I looked at Mr. Ton-That through the glasses, a green circle appeared around his face. I tapped a touch pad at my right temple. A message came up on a square display that only I could see on the right lens of the glasses: “Searching …”

And then the square filled with photos of him, a caption beneath each one. I scrolled through them using the touch pad. I tapped to select one that read “Clearview CEO, Hoan Ton-That;” it included a link that showed me that it had come from Clearview’s website.

I looked at his spokeswoman, searched her face, and 49 photos came up, including one with a client that she asked me not to mention. This casually revealed just how intrusive a search of someone’s face can be, even for a person whose job is to get the world to embrace this technology.

I wanted to take the glasses outside to see how they worked on people I didn’t actually know, but Mr. Ton-That said we couldn’t, both because the glasses required a Wi-Fi connection and because someone might recognize him and realize immediately what the glasses were and what they could do.

It didn’t frighten me, though I knew it should. It was clear that people who own a tool like this will inevitably have power over those who don’t. But there was a certain thrill in seeing it work, like a magic trick successfully performed.

A lost opportunity?

Meta has been working for years on its own augmented reality glasses. In an internal meeting in early 2021, the company’s chief technology officer, Andrew Bosworth, said he would love to equip them with facial recognition capabilities.

In a recording of the internal meeting, Mr. Bosworth said that leaving facial recognition out of augmented reality glasses was a lost opportunity for enhancing human memory. He talked about the universal experience of going to a dinner party and seeing someone you know but failing to recall their name.

“We could put a little name tag on them,” he said in the recording, with a short chuckle. “We could. We have that ability.”

But he expressed concern about the legality of offering such a tool. Buzzfeed reported on his remarks at the time. In response, Mr. Bosworth said that face recognition was “hugely controversial” and that granting broad access to it was “a debate we need to have with the public.”

While Meta’s augmented reality glasses are still in development, the company shut down the facial recognition system deployed on Facebook to tag friends in photos and deleted the more than one billion face prints it had created of its users.

It would be easy enough to turn such a system back on. When I asked a Meta spokesman about Mr. Bosworth’s comments and whether the company might put facial recognition into its augmented reality glasses one day, he would not rule out the possibility.

The post The Technology Facebook and Google Didn’t Dare Release appeared first on New York Times.