Hot Clicks: Is Google Letting People Read Your Emails?

Rounding up IT and advanced tech-related news impacting government and industry.

Amanda Ziadeh

Mon, 07/09/2018 - 16:27

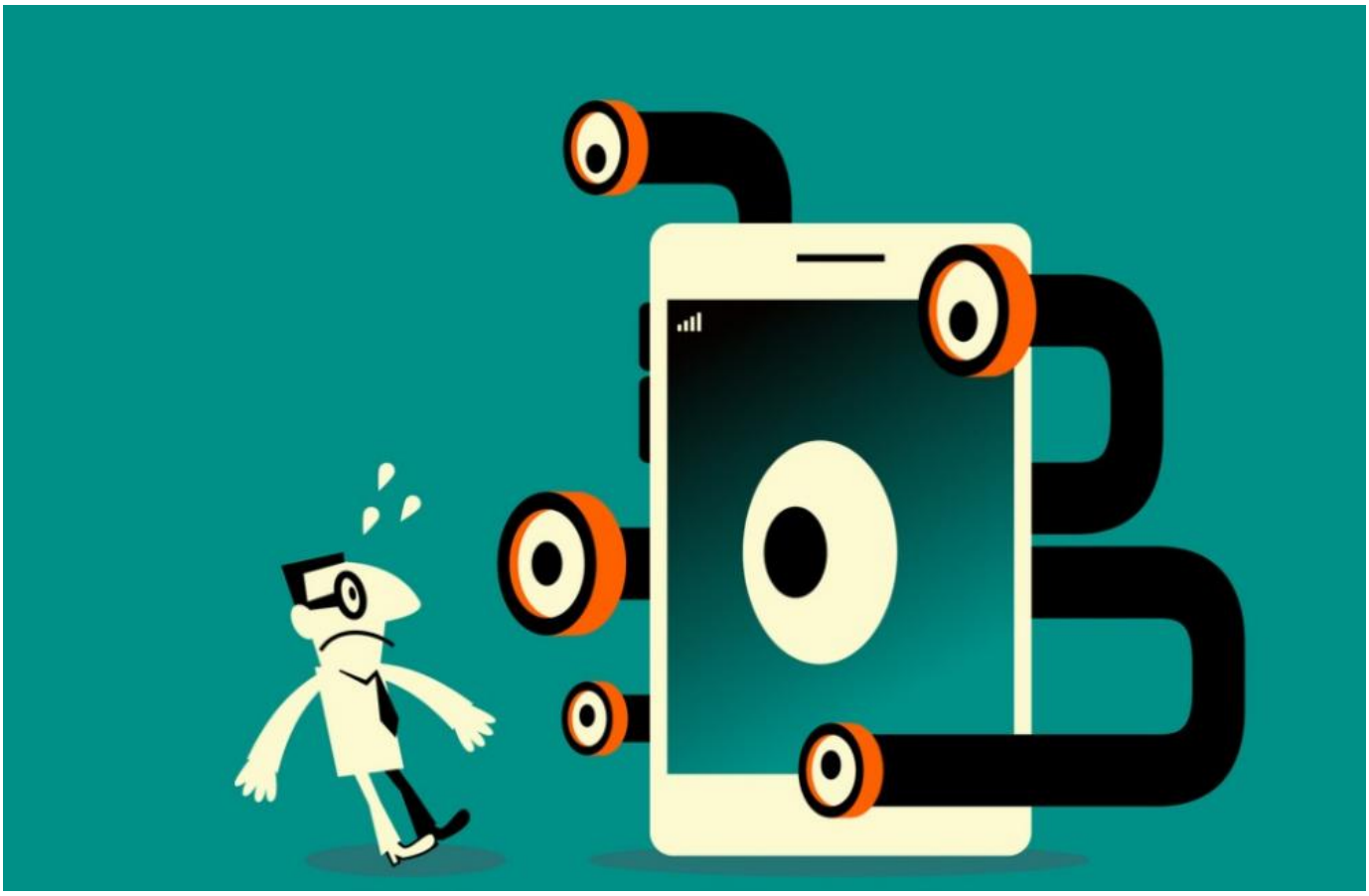

Illustration: alashi/iStock

Another day, another breach of consumer privacy and trust. Despite GMail user privacy promises Google made a year ago, the Wall Street Journal reported that the tech giant has been letting hundreds of outside application and software developers scan millions of inboxes. Specifically, these app developers were allowed to access the inboxes of users who signed up for tools like price comparisons or travel itinerary planners. So, by downloading that tool and opting in, users were unintentionally exposing their own Gmail messages and email information to third

parties.

It’s not just artificial intelligence or computer programs scanning inboxes, either. According to the Journal, in some cases, human employees at the third party companies have been scanning users’ GMail, too. And the consent form that users are signing to allow outside apps to scan their emails doesn’t necessarily say humans might be doing it too. But don’t worry, Google said they vet all outside developers they provide data to, and their own employees only read emails for security purposes and when given consent by the user. NBC News

Artificial Neural Network Created with DNA

Researches at the California Institute of Technology created an artificial neural network from synthetic DNA, and it’s pretty smart. The neural network can recognize numbers coded in molecules, but what does creating it from DNA even mean? Well, neural networks are a type of computing architecture based on the human brain, and they’re fed a lot of data and taught how to perform tasks with that data, leading to machine learning. Caltech researchers designed this, but instead of using silicon and transistors for the neural network’s hardware, they used DNA and test tubes.

Here’s how it works: strands of DNA’s four basic nucleotides — Adenine, cytosine, guanine and thymine — can bind with each other to form the double helix of DNA, but only in specific combinations, and the pattern of combination makes the nucleotide strands perfect for computing devices. These DNA-based computing devices can then be designed to produce certain chemical reactions when in the presence of different molecules. So, the Caltech researchers tested their DNA-based computer with teaching an algorithm to recognize handwritten numbers. They fed the artificial neural network a bunch of handwritten examples of a number, and the algorithm learned to generalize the qualities from different examples to form an idea of what a specific written number looks like.

Essentially, the neural network can look at a four written by a human, and conclude that it is, indeed, a four. The test tube shows a fluorescent signal to indicate the networks’ decision. Motherboard

Smartphones May Not be Listening, But They're Watching

A few computer science academics at Northeastern University wanted to know if the technological theory that our smartphones are always listening to us was really true or not, so they conducted a year-long experiment that involved 17,260 of the most popular apps on Android. They wanted to know if any of those apps were secretly using the phone's mic to snag audio, but actually found no evidence of apps activating the mic or sending audio on its own. What they did find was that apps were recording a phone's screen and sending that information to third parties.

Of all the apps in the experiment, more than 9,000 of them had permission to access the camera and microphone. The researchers used 10 Android phones and an automated program to interact with the apps, and then analyzed the traffic generated looking for any media files that were sent to an unexpected party. But rather than audio files, they found that screenshots and video recordings of what people were doing in the apps were being sent to third party domains. So, for example, when one of the phones was using an app from GoPuff, a delivery start-up, the interaction (including the input of personal information) with the app was recorded and sent to a mobile analytics company. Gizmodo

China's Tech-Powered Authoritarian Future

China has an estimated 200 million surveillance cameras, which is four times as many as the U.S. In cities around the country, police officers wear facial recognition glasses to spot drug smugglers, AI-powered cameras are used to find criminal suspects in large crowds or stores, cameras scan populated areas like train stations for criminals, and large public displays of outdoor screens show the faces and names of jaywalkers or people who can't pay their debt. Beijing is using the same kinds of technologies to identify and track its 1.4 billion people, as the country aims to build a national surveillance system.

And this is along with China's other tech systems that track things like internet use, communication and travel bookings. The same technology isn't used in all the cities yet, so the nationwide surveillance network isn't quite there yet, but the threat

certainly is. Martin Chorzempa, a fellow at the Peterson Institute for International Economics, called this new way of managing society “algorithmic governance.” This way of ruling is breaking down previous societal agreements between the Chinese government and its citizens as technology and surveillance are used for power and limiting privacy. The New York Times

New Robot Algorithm Replaces Vision with Touch

This is the reality for Massachusetts Institute of Technology’s 90-pound Cheetah 3 robot, which is navigating its environment by touch, and running up stairs without needing to actually see the stairs. Other robots are capable of walking up steps with the use of a camera, but Cheetah’s developers think relying too much on vision could slow the robot down. For example, stepping on something that the camera didn’t see can make it stumble. So, the designers are using “blind locomotion” so that the robot doesn’t solely trust its vision, and can explore potentially dangerous areas that humans can’t.

The team used algorithms and sensors to provide the robot with proprioception, the sense of knowing where its body is in space. Cheetah 3 also has upgrades to its hardware so it can stretch and twist, and predictive algorithms that help it change its gait so it doesn’t trip or fall. In the video from MIT, the robot is shown running up the stairs, twisting and wiggling, prancing, and bending its invertible knee joints the wrong way. Ultimately, a robot like this could be used to go inside power plants for inspections or deep in environments where it may not be able to see, but can still complete the task. The Verge

View printer friendly version
news roundup
Google
AI
robots
China
machine learning
MIT
surveillance