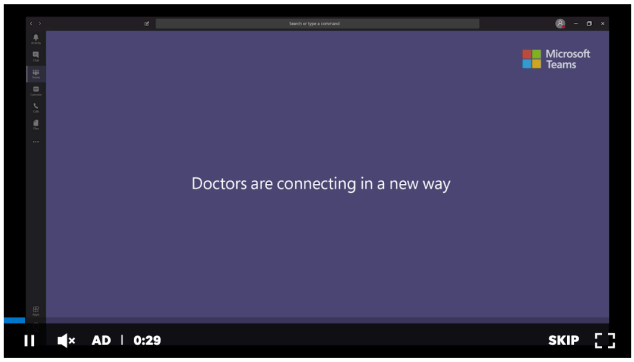
TECH

5G is speedy, but does it also raise the stakes on privacy, security, potential abuse?

Edward C. Baig USA TODAY

Published 12:11 p.m. ET Mar. 27, 2019 | Updated 9:59 a.m. ET Mar. 28, 2019



This button on your microwave will give you much better cooking results

The microwave is one of the most common kitchen appliances but there's a really useful button you might not be using....

USA TODAY

stakes on privacy, security, potential abuse?

Edward C. Baig USA TODAY

Published 12:11 p.m. ET Mar. 27, 2019 | **Updated 9:59 a.m. ET Mar. 28, 2019**

Story Highlights

Experts believe that 5G is more secure than the networks that have come before.

Under the more sinister scenarios, consumers may not even know what hit them.

Sure, the next generation of wireless will bring you faster phones, smarter tech and seamless services. But could 5G also make your privacy vulnerable?

While you often hear that 5G promises to eventually rev-up health care, self-driving cars, virtual reality, even entire “smart” cities, what you don’t hear quite as often is how it raises the stakes on privacy and security.

"5G implies faster speeds for good guys and for bad guys," reminds Galina Datskovsky, CEO of Vaporstream, a secure messaging company in Chicago.

But before we let our fears and concerns move too far ahead of us, let's take a step back. What does this really mean?

From the increasing use of artificial intelligence to connecting networks of devices at home to more secure ways to track transactions, “There’s a whole series of related technologies happening all at once,” says Mark Foster, senior vice president, IBM services and global business services. “Each has their own risks with regard to security, privacy and how they operate. In the end, it’s about the ethical operation of all this stuff.”

With the dramatic proliferation expected of network-connected 5G devices, “governments will need to test these systems carefully before they are deployed," says Marc Rotenberg, president of the Electronic Privacy Information Center. "And end-to-end encryption for network traffic should be a priority."

Verizon 5G to go live: Verizon's mobile 5G network goes live on April 11, starting in Chicago and Minneapolis

USA TODAY

Fear mongering is surely not justified, and experts, in fact, believe that 5G is more secure than the networks that have come before. But 5G alarm bells have been sounded nevertheless, and some degree of vigilance is prudent.

This past fall, a team of international researchers determined that while 5G data protections have improved compared to predecessor 3G and 4G LTE wireless networks, “critical” security gaps remain.

The potential for 5G abuse

“What if 5G dashcams, bikes, suitcases, umbrellas, garments, etc. become a thing?” asks one of those researchers, Sasa Radomirovic, senior lecturer in information security at the University of Dundee in the U.K.

“For each 5G equipped thing, there will be the possibility that an attacker or manufacturer abuses it to invade your privacy.”

The flip side, of course, is that a manufacturer can also use the connectivity to improve your service, Radomirovic notes.

But attackers, he says, might exploit everything from mining Bitcoin to posting fake news on Twitter. Even creepier: a cyber-intruder might eavesdrop through a 5G baby-cam.

Dan Garraway, a co-founder of an interactive video technology company Wirewax, sees another possibility brought about by 5G. While you are watching video content that is being distributed via 5G, you might be watched back.

Smart TVs have been collecting data on your viewing habits for some time now. In 2017, TV maker Vizio was forced to pay $2.2 million to the Federal Trade Commission and the State of New Jersey because it was snooping on viewers without their consent.

How such practices play out in an interactive 5G viewing environment will depend on how companies go about it, which ones partake, and whether the consumer has a say in the matter.

“If, for example, Netflix decided to do something and was very obvious about it and gave the viewers the benefits of what they would get in return – and there was an opt-in – then people probably would trust it," Garraway says.

Under any of the more sinister scenarios, consumers may not even know what hit them.

Current mobile attacks, says Vivien Raoul, chief technology officer at global security firm Pradeo, mostly operate silently in the background. “Often, the only visible sign is a system slows down. 5G will make it harder for end-users to notice they are being attacked.”

For his part, Columbia University computer science professor Steven Bellovin takes a different perspective. He worries that mobile carriers will be able to detect your whereabouts more precisely because the shorter range of the initial wireless 5G signals will, he says, necessitate more cell towers that are closer to your location.

But Bellovin says the real risk comes not from the network itself but potentially from applications that would not have been possible prior to 5G. "We'll certainly see new things having to do with networking in cars," he says by way of example. "Is this going to be a huge privacy issue? I'm not sure. The question is how large an increment is it for privacy over the things they already know?"

On the world stage, there are other subplots that bear scrutiny. For instance, citing espionage fears, U.S. lawmakers have expressed major concerns about Chinese telecommunications giant Huawei and its ambitious plans to lead globally on 5G. Huawei has not only denied the allegation but has sued the U.S. government over a federal ban against the Chinese maker's equipment.

Just this week, the European Union recommended a series of steps in which member nations assess their own 5G risks by the end of June and collectively work thereafter to ensure a high level of cybersecurity. The EU resisted U.S. pressure to impose a similar ban against Huawei.

Recent high-profile security ruptures and the misuse of data have already put consumers on edge. According to IBM Research, 81 percent of consumers globally say that in the past year they have become more concerned with how companies are using their data. And 75 percent are less likely to trust companies with their personal information.

How the industry is addressing privacy and security

To be sure, the wireless industry isn’t taking privacy and security lightly.

are extending the security of 5G wireless networks to other networks – called home network control – when a user is roaming or using a network like Wi-Fi.

What's more, the providers are increasingly deploying network components that are virtual instead of the hardware of yesteryear. That means cloud-based network systems can be adjusted, removed, or replaced using software on the fly and in real time.

Ana Tavares Lattibeaudiere, head of North America for another mobile communications industry trade group, the GSMA, says while the fact that everything will be connected "brings unprecedented opportunity, it also brings into focus the huge amounts of data that will be going over the networks."

"For consumers, it may seem like a choice between sharing their data and hoping for the best, or keeping it private and secure but missing out on the connected experiences. The telecommunications industry and service providers should not only think about network and infrastructure security – which are highly important – but also how 5G can bring in an era of user choice."

Along those lines, the GSMA has developed a digital authentication standard called Mobile Connect, which essentially allows users to create and manage a universal digital identity via a single login. By matching a user to their mobile phone, Mobile Connect allows them to log-in to websites and applications quickly without the need to remember passwords and usernames. The GSMA claims this will strengthen cybersecurity and reduce the risk of data breaches.

Radomirovic says that the security flaws researchers recently discovered were serious but will be fixed. "What we remain concerned about are the less-than-perfect privacy protections 5G provides leaving users vulnerable to targeted attacks."

As 5G rolls out, it is very likely fresh safeguards, tools or updates to security software will emerge to help consumers protect their privacy, at least under some circumstances. In any burgeoning environment, it always makes sense to keep your guard up.

Email: ebaig@usatoday.comFollow @edbaig on Twitter