What will it take for the government to protect your privacy?

January 21 2020, by Edward C. Baig

Credit: CC0 Public Domain

Is 2020 the year when the government finally does something real to protect your privacy? Up until now, it has been all on you, the consumer.

When it comes to today's technology, it's not just Big Brother watching

or even Big Tech. Your Fitbit tracker, Ring camera, Alexa voice assistant, Google searches—almost anyone seems to have access to the data of your life.

"You have zero privacy anyway." That's how then-Sun Microsystems CEO Scott McNealy put it to reporters and analysts more than a couple of decades ago.

But should we get over it?

A majority of Americans believe it is not possible to go through their daily lives without being tracked, according to a recent Pew Research study.

While we've grown accustomed to it, is that really something we should simply accept?

"Just the fact that almost every day when we read the newspaper (and) see different concerning stories about privacy and security breaches, it would be almost impossible to conclude that enough is being done, said Federal Trade Commission commissioner Rebecca Slaughter, speaking during a privacy panel at the recent CES tech industry expo in Las Vegas. (She said the opinions were her own and not that of the FTC.)

So the question is whether this year will finally be the one that puts some legal heft behind consumer privacy protections.

U.S. lawmakers certainly lag their European counterparts. The EU's General Data Protection Regulation, more commonly referred to as GDPR, went into effect in 2018. In this country, only California, whose own new privacy law took effect Jan. 1, appears to be tackling this issue head-on.

Other states are all over the map when it comes to laws governing online privacy, according to rankings from the Comparitech security and privacy research firm.

Still, debate continues about whether the U.S. needs a privacy law that covers all 50 states.

"We would like to see a national law around this," said Amazon senior vice president for devices and services David Limp during an interview at CES. "Because trying to implement it state by state, with nuances in every state that are slightly different, leaves a lot more room for subjective interpretation."

To be sure, the Feds haven't been completely neutered. Just this past July, the FTC fined Facebook $5 billion, a record-breaking sum that was part of a settlement for violating consumer privacy, prompted by the 2018 scandal involving Cambridge Analytica. Though it was not the only data rupture to stain the company.

At CES, Facebook vice president and chief privacy officer Erin Egan conceded that more needs to be done, while talking up the social network's recently expanded privacy checkup tool for consumers.

Her counterpart at Apple, senior director for global privacy Jane Horvath—the public appearance by an Apple executive at CES was a rarity—reiterated the company's long-standing commitment to "privacy-by-design" principles used across all its products.

But she agreed that "there's no way to say that at this point in time we've reached a panacea."

While the tech industry appears to be saying all the right things—and in some instances doing something about it—critics still aren't persuaded.

Washington Post columnist Geoffrey A. Fowler calls such statements "privacy white-washing: when tech companies market control and transparency over data but continue gobbling it up." It's not what we need, he says.

Amazon and Google's ring of privacy fire

The devices and services we have given free rein in our homes and our lives to make things easier have, in too many cases, become portals to privacy violations instead.

Amazon-owned Ring came under fire in December after login names and passwords of more than 3,000 customers were exposed. There have also been frightening reports of hackers compromising the Internet-connected cameras and doorbells.

A family in Mississippi had claimed that a hacker gained access to a Ring camera placed in their 8-year-old daughter's room and started talking to her.

Ring said at the time that the incident was not related to a breach or compromise of its security but rather due to the fact that customers often use the same username and password for their various accounts and subscriptions, which bad actors may obtain elsewhere.

Still, regarding Ring, Amazon's Limp insists, "we've had very good security in place, including what I would consider best-in-class two-factor authentication."

But, he added that in some cases, "we needed to be more strict on the path (customers) took to put high security in place. So instead of an option of two-factor authentication moving forward, we're going to make it mandatory, a lot like your bank does."

He also said that Amazon enabled a feature over the holidays that any new log-in attempt on a device that you already have installed will send you a notification to put in a code.

Always alert Alexa and Google Assistant have been caught listening when you might not have expected them to be, which wigs out many consumers. Amazon has long insisted its voice assistant is, essentially, holding its breath until it detects the "Alexa" wake word.

Limp claims Amazon is being more transparent nowadays. For example, Amazon added an Alexa privacy dashboard portal, and you can now tell Alexa to "delete what I just said." You can also opt out of "human annotation," where Amazon employees are able listen to voice recordings, in an effort to make the system better. Limp says only a fraction of 1% of data is seen by human eyes, and all personally-identifiable information is removed from such recordings anyway so that Amazon doesn't know that it is you.

Now, if you do nothing, he says Amazon will keep your data in perpetuity.

Google also recently added the ability to tell its Assistant to butt out by saying, "Hey, Google, that wasn't for you," which is supposed to give the Assistant a temporary case of amnesia.

Protecting privacy is on you

Still tech companies don't make it easy for the consumer.

"I'm a relatively well-educated person who specializes in privacy," Slaughter said, "and I can't possibly figure out all the things that are being done with all my data across different services. And that's just by the companies with whom I have a first-party relationship and doesn't

even think about the backbone infrastructure where there's third-party data sharing."

A network of data or information brokers collect, buy or sell your personal information, typically without your knowledge. This largely unregulated industry is said to be worth more than $200 billion.

Almost no one reads a tech or other company's terms of service. Even if you do, you may need legal training to figure out what it all means.

Beyond the short-term violation of one's privacy, Slaughter frets about the "downstream harms," decisions based on leaky data about your future job or credit prospects, for example, or "the targeting of content to consumers in ways that could be manipulative or problematic."

And what's abundantly clear, tech evolution isn't just the domain of the well-meaning. "With every advancement in technology, the people who want to do bad things get more sophisticated as well," said Jeff Immelt, the longtime head of GE who is working with smart home platform Tuya, though he did tell U.S. TODAY that he believes the good guys are keeping pace.

In the meantime, Apple's Horvath rattled off some of the ways it strives to protect customer privacy. For example, the company creates random numerical identifiers to mask data sent up to Apple's servers when you use Siri or Maps.

Apple adheres to the mantra that privacy is a human right and also uses the company's stance on privacy as a marketing tool.

But Apple's position also leads to friction with law enforcement when investigators seek access to evidence locked away in a privacy-infused device.

Amid all of this, one thing is apparent: It will take a lot more industry efforts—combined with stricter Federal intervention—to give consumers the data safeguards and level of privacy that ought to expect and so richly deserve.