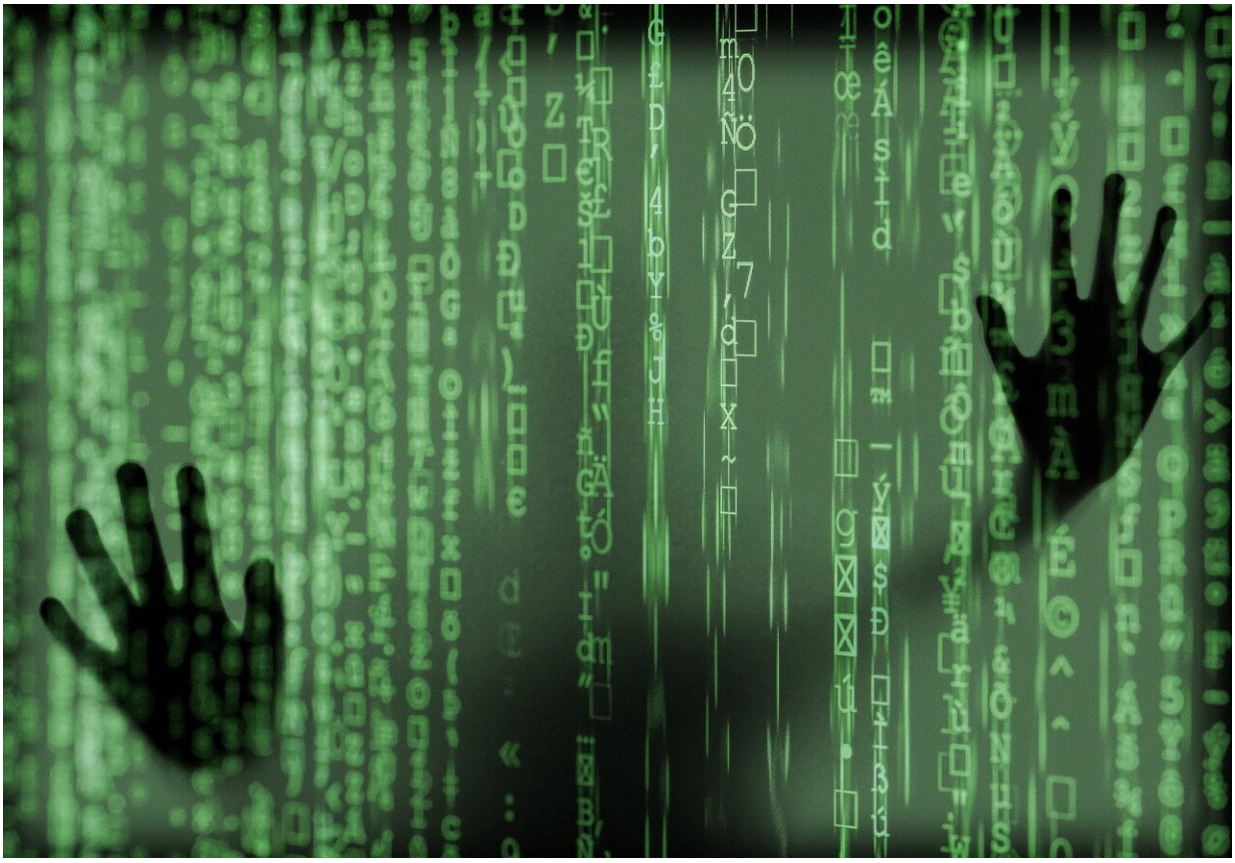
How technology made us bid farewell to privacy in the last decade

December 24 2019, by Jefferson Graham



Credit: CC0 Public Domain

In 2011, Apple unveiled its first iPhone with artificial intelligence, a personal assistant named Siri that could answer questions and help keep track of our daily lives.

The AI revolution had begun, and it gave way to higher resolution cameras on phones, such as the then-new iPhone 4S, microphones and cameras in the home, everything from connected speakers, security devices, computers and even showers and sinks.

By the end of the decade, we were carrying and or living with devices that are capable of tracking our every movement.

Counties and states are selling our personal information to data brokers to resell it back to us, in the form of "people search engines." Facebook and Google have refined their tracking skills, in the pursuit of selling targeted advertising to marketers, that many people believe they are listening to us at all times. They are that good at serving up ads based on our interests, whether we want it or not.

Goodbye privacy!

The "10s" were the decade in which our privacy went away if we were connected to the Internet, which means most of us. Apple went on a crusade to protect our privacy, which could be argued as a competitive advantage over rivals, and groups ranging from the Electronic Frontier Foundation (EFF) and the Privacy Coalition began speaking out. In Europe, major changes were made to privacy laws on behalf of consumers, and a new California law goes into effect in January that will make it harder for companies to take our data and resell it.

Or so the language says.

As more people became aware of privacy issues, and companies like Facebook announced several security breaches of our data, the bottom line is that the social network has more users and makes more money. Ditto for Google.

"The biggest difference between then and now, is that people didn't really think about what companies were collecting on us," says Chris Jordan, CEO of Fluency, a data analysis company. "We weren't worried about privacy. Now we are."

Not that it wasn't brought to our attention. In 2011, then hacker/security researcher Samy Kamkar discovered that the iPhone, Android and (the then still operating) Windows Phone mobile devices were sending back GPS information to their makers, even when the location services option were turned off, and made his findings public.

Bluetooth is always on, despite the settings

In 2019, Kamkar demonstrated for a U.S. TODAY reporter how little has changed. From the general settings of the iPhone, turn off the blue bluetooth icon in the Control Panel, and then go to the Bluetooth section in General, and Bluetooth is still running.

"When you disable, you're not disconnecting the software that continues to broadcast the information," says Kamkar, who is now the chief security officer and co-founder of Openpath, a company that aims to replace the office badge with app-based tokens for entrances. "I can still get your name and phone number simply by being in the vicinity," and picking up the bluetooth signal.

And there are more sensors reading you than ever before. Google now tracks your every movement, if you're a user of the Google Maps smartphone app, and records a public history of your whereabouts, whether or not the app is even open and turned on.

"We knew we were being tracked on phones, but didn't realize that the companies were using the data in ways most people don't approve of, or even realize it was capable of," says Danny O'Brien, director of strategy

for the EFF.

Privacy concerns went from something people were "benign about, to genuinely anxious," he adds.

Just ask comedian/actress Tanjareen Martin Thomas.

Cover your webcam and your phone

"Most people cover their webcam cameras, but don't think about the phones," says Kamkar.

Thomas does. She brings her phone to the bathroom, but always places a lens cloth around the cameras.

"I don't want some stranger watching me change my clothes," she says. "I cover everything."

From the bathroom to the living room, the major innovation in TVs over the decade has been the smart TV, which eliminates the need for an external streaming device to bring internet programming from the likes of Netflix, Hulu and Disney+ direct to the set, without having to change the HDMI input settings.

The sets themselves got so cheap, resellers are practically giving them away, with many Black Friday deals offering 40- and 50-inch models in the $200 and $300 range. These same size sets were selling for around $1,000 in 2010.

How to make money selling TVs—resell our data

That's the good news. The bad: to turn a profit, manufacturers now make

up the difference by selling your viewing habits to data brokers, letting them know what shows and networks you watch, your demographic and real estate locations and more.

Samsung has a TV with a built-in video camera, to enable video chat, but it also makes the TV even more susceptible for hacking. The onus is on the consumer to protect their smart devices with strong passwords, especially for the home network.

Which brings us to the ever-present security doorbell cameras that are increasingly showing up in people's homes. Ring, a company owned by Amazon, has come under attack by privacy groups for being allegedly easy to hack, not just for the doorbell product.

The group Fight for the Future put out its own product warning, saying Ring cameras are not safe. Recently, several families have reported that their Ring cameras were hacked. In response, Ring said its owners needed to use stronger passwords.

Meanwhile, as we close off the decade, yes, people are fighting back against the privacy invasion, politicians have taken up the cause, with a vow to break up big tech, but what will it all look like in another 10 years. There's artificial intelligence and facial recognition to add to all the tracking that's going on now.

The age of "Minority Report," the sci-fi novel and film where government could pre-determine what you were going to do with visions of the future "will happen," says Kamkar. "It's just a question of how far we'll let it go."

(c)2019 U.S. Today
Distributed by Tribune Content Agency, LLC.

Citation: How technology made us bid farewell to privacy in the last decade (2019, December 24) retrieved 10 April 2024 from https://techxplore.com/news/2019-12-technology-farewell-privacy-decade.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.