

## You are being watched (Does it matter?)

Posted At : July 31, 2020 9:32 AM | Posted By : Admin

Related Categories: Workplace

We are being watched. This isn't paranoia—in the past year we've seen dozens of headlines warning us that our personal data is being collected, even as the CEOs of Big Tech argue that our interests and preferences are safe on their platforms. "We don't sell people's data, even though it's often reported that we do," Facebook's [Mark Zuckerberg](#) wrote in the Wall Street Journal. "We've stayed focused on the products and features that make privacy a reality—for everyone," Google's [Sundar Pichai](#) later penned in the New York Times.

But can data privacy even exist in a world where the data we produce is being constantly monitored? Most people understand and accept that if you search Google for a new hairbrush, you may start seeing hairbrush ads. But what about Google marketing to you by scanning your FitBit data (which [Google now owns](#)) or accessing your medical records (as they did with their controversial [Project Nightingale](#))? And what happens when medical professionals need to access your records and are told you don't own that information anymore?

### How Americans view surveillance

If you feel like you're under surveillance, you're not alone. [A study of 4,272 Americans by Pew Research](#) shows that most people don't like their data being collected but don't know how to stop it:

- 6-in-10 people think that both businesses and the government are collecting their personal data on a daily basis
- 8-in-10 feel like the data collection is out of their control
- A majority don't understand what is being done with their data
- Social media and smart speaker data collection had the lowest approval rates
- Conversely, data sharing that was done for a specific purpose—such as sharing student data to improve schools, or collecting data to avert terrorist threats—garnered positive approval ratings

While these numbers aren't surprising, they also show how big tech companies haven't assuaged our worries about trading off our personal information for online conveniences, such as Amazon logins on third-party sites. In fact, a majority consider data collection very risky:

- 81% think the risk of companies collecting their data outweighs the benefit
- 66% feel the same way about government-collected data

### Behavioral biometrics and ethical issues

How about companies that monitor your behavioral biometrics, such as how long you pause on a web page, or your typing patterns, or how happy (or mad, or frustrated) you sound when you ask your voice assistant a question? (Last summer Jeff Bezos admitted to congress that Amazon holds on to your voice data [even after you delete it.](#)) With the behavioral biometrics field growing at a [23.7% a year](#), your every move is valuable and can be sold to the highest bidder.

But just like your other personal data, do the companies who monitor you own it, or do you? What if you don't even know you're being monitored? Here are a couple of the surprising ways your data is being collected.

- Modern connected cars have the power of 20 personal computers, according to a McKinsey survey. The data it gathers isn't only about vehicle performance, either—it can monitor things like how fast you drive or how hard you hit the brakes. Some can even ID you via [sensors in your seat](#) (and yes, they'll notice if you've gained weight).
- [Walmart has patented a shopping cart](#) that can monitor your heart rate, grip force, palm temperature, and walking speed as you wheel it around the store. The sensors in the cart connect to a server which then notifies employees to check on customers that hit certain thresholds.

## Why privacy should matter to businesses

The GDPR has affected large US businesses with international reach, and state-level laws such as the [California Consumer Privacy Act \(CCPA\)](#) exempts businesses under a \$25 million threshold—which means small- and mid-sized businesses haven't been hugely affected yet. But with the possible implementation of a [federal privacy law](#) in the near future, you should have a plan in place for the way you gather and safeguard your customers' and employees' information. Here are a few reasons why:

- **It's important to your current customers.** As the Pew Research survey showed, it's a high priority for the majority of Americans. If you make it clear to your users that they own their own data, it can also serve as a good retention tool for your current userbase.
- **It separates you from the competition.** If you are transparent about your data gathering, usage, and customer ownership—and your competitors are not—it can attract new customers and business partners.
- **It looks good for employee recruitment.** In a competitive recruiting landscape for tech employees, demonstrating that you are an honest company that uses consumer data ethically makes you stand out.