The Christian Science Monitor

Snooping? Companies do it, too.

It's not just the National Security Agency that's watching you. From building a profile of the type of consumer you are to watching what you click on and how long you browse a website for, companies are tracking your every move, experts say.

By: Akane Otani - August 12, 2013

Recent revelations that US surveillance programs collected the data of millions of people using Google, Facebook, and other Internet services have shocked many Americans and caused a backlash in Congress that may lead to stricter oversight of government snooping. But for most Americans, the bigger threat to their privacy lies in the commercial world.

Every day, companies buy, amass, and study consumers' digital footprints to identify who they are and what they will buy. The profiles they build are so sophisticated that they:

> •Reduce consumers' bargaining power. Each month, Dataium, which describes itself as "the world's largest compiler of online automotive shopping behavior," tracks more than 20 million consumers browsing automotive websites. Recording mouse clicks, Dataium tells companies what brand, model, and even trim level of car a particular consumer is looking at, says Justin Brookman, director of consumer privacy at the Center for Democracy & Technology. When customers walk into a dealership, the salesman can find out what they know – and don't know – about the model they are considering.
>
> •Adapt in the blink of an eye. Just as you begin shopping for new shoes online, Facebook shows you a shoe ad. Coincidence? Hardly. Advertisers follow consumers from one website to another, bidding in milliseconds for the right to show ads to specific consumers.
>
> •Can lock out customer options. Do you return lots of merchandise to stores? On the lookout for fraud, retailers track how often customers make returns. If you seem to return too often, they may trigger exceptions in their return policy and refuse to refund your money. They can even keep you from shopping at their stores.

The profiles are so detailed that, in a practice assailed by critics as a gross violation of privacy, companies can buy lists of people with specific characteristics: millionaires in the United States, people with poor credit histories, or even adults with a condition diagnosed as Alzheimer's, says Jay Stanley, senior policy analyst with the privacy and technology project at the American Civil

Liberties Union. "The full genius and fury of American capitalism is being used to figure out how to better surveil Americans," he says.

In many instances, data collection helps consumers. A retailer that tracks its customers can anticipate what they might like and present it to them online or alert them to sales for products they have searched for in the past.

"Should we be concerned that sites like Amazon are gathering information for the purpose of telling us what we might like?" asks Julian Sanchez, a research fellow at the Cato Institute, a libertarian think tank in Washington. "I'm not particularly troubled by it, but Amazon is also fairly transparent about what they do with your information."

The problem with consumer tracking comes when companies begin to share information with others. Sometimes, they do so unwittingly. Hackers repeatedly tap into company computers to steal credit-card numbers and other customer information. Sometimes companies are forced to give up the data when the government requests it, as the leaked files of the National Security Agency revealed earlier this year.

What's most troubling to privacy advocates – in an eerie parallel with the NSA spying programs – is the sheer volume of information companies are gathering. The masses of data work for their own profit – not consumers' benefit, privacy advocates say.

"It increases their power over you," Mr. Stanley says. "This is largely being done outside of the public's eye, and the amount of information that is being collected is far outside of the balance to provide the kinds of benefits – telling people what they might like to buy – that people talk about."

Neither the government nor companies are always candid about who and what they track. And the US has very few restrictions on sharing data with third parties, says Ashkan Soltani, an independent researcher who has advised the Federal Trade Commission (FTC) on privacy issues. There's also "very little people can do in the digital world to protect their communications."

While consumers can pay for their purchases in cash, reduce their cellphone usage, and try to encrypt their messages to maximize their privacy, Mr. Brookman says it is unfair to place so much of the burden on consumers.

Privacy advocates have made some strides in restricting surveillance. After a 2012 investigation concluded that Facebook deceived its users, the FTC corralled Facebook into getting express consent from consumers before changing their privacy preferences. Facebook also has to undergo audits of its privacy programs twice a year for the next 20 years. But the road to reclaiming privacy is steep.