The data backlash: Privacy

Ashley Carman

May 1, 2015

Americans have questions, and they want answers.

Thanks to former National Security Agency (NSA) contractor Edward Snowden exposing the U.S. government's penchant for data, and recent documents revealing the way law enforcement uses stingray devices to often collect innocent civilians' data, Americans are pushing their government, technology providers and anyone with access to their data for answers and accountability.

Plus, mounting evidence that living under the threat of surveillance is changing online habits and possibly stifling creativity is now prompting companies to modify products and change their approach to privacy.

A pair of Pew Research Center studies illustrates Americans' privacy woes. Research from November 2014 found that 91 percent of adults “agree” or “strongly agree” that consumers have lost control over how personal information is collected and used, and 80 percent agreed or strongly agreed that Americans should be concerned about the government's monitoring of phone calls and internet communications.

A second study from March of this year shows just how those beliefs translate into tangible behavior. Twenty-two percent of American adults say that since the Snowden revelations they've changed the patterns of their own use of various technological platforms “a great deal” or “somewhat.”

That's not good news for a digital society where personal lives and business thrive on the flow of information, and innovation depends on people having the freedom to explore and work without government peering over their shoulders. While the percentage of people who've adjusted their

online habits isn't a majority, it still represents more than 50 million Americans and doesn't even take into account the vast majority of Americans who are simply aware of government surveillance, or 87 percent of adults.

"These are huge numbers," says Omer Tene (*left*), vice president of research and education at the International Association of Privacy Professionals. They also demonstrate a privacy awareness that "certainly wasn't the case before the whole Snowden NSA story got out."

He explains that in the wake of those revelations, American society has seen a "spike in knowledge, awareness and interest from consumers and, correspondingly, from businesses that have to react to consumer sentiment."

Patrick Eddington, policy analyst in homeland security and civil liberties at the Cato Institute, a public policy research organization, agrees, positing that the world is seeing a "digital resistance movement."

That resistance is apparent in *Citizenfour*, a documentary about Snowden's leaks. When discussing the documents he's downloaded from the NSA, Snowden takes care to avoid eavesdropping by unplugging his hotel room's phone. It's almost cringe-worthy paranoia. While most of us aren't Snowdens with a specific reason to worry about government surveillance, his concern and care seemed to preview the future of privacy and the lengths to which citizens might have to go to preserve theirs.

With 54 percent of Pew Research respondents believing it would be "somewhat" or "very" difficult to find tools and strategies that would help them be more private online and with their cell phones, duct tape over a webcam can't be ruled out. But more thoughtful – and feasible – alternatives exist.

The lack of knowledge around privacy options "is an indication that public education needs to take place," says Eddington (*right*). "There are excellent privacy tools out there, and they're getting easier to use with each passing month."

For instance, the Blackphone, a privacy-driven mobile device from Silent Circle, features apps, including two that encrypt both phone calls and text messages, that attempt to give users control over their data.

"All of the sudden there's this manifestation of all those [privacy] fears being realized across what we're doing," says Bill Conner, CEO of the Switzerland-based encrypted communications firm. Public discomfort with privacy issues is driving interest in his firm's platform, he says.

A number of companies beyond Silent Circle are rising up to fill the void where the government and its policies have failed, Eddington says, but even more than new products being created with privacy in mind, companies are attempting to gain back users' trust with their own privacy deployments. It's not a surprising move given that 81 percent of Americans feel "not very" or "not at all secure" using social media sites when they want to share private information.

Yahoo, for example, met consumers' call by saying it would begin rolling out end-to-end encryption for its email users. WhatsApp implemented encryption on users' messages last year and transparency reports – proffered by the likes of Google, Twitter and Facebook to show data requests from government and law enforcement – have been presented as evidence that social media firms are trying to keep their customers in the know. These companies are focusing on reestablishing relationships with users based on trust as opposed to forging new ones. To that end, they're looking into roles beyond a privacy officer.

“It's evolving into a question of trust,” says J.J. Thompson, CEO and managing director at Rook Security, an Indianapolis-based provider of global IT security solutions, hailing “the creation of trust officers who bridge privacy and security and brand under one umbrella.”

This recent change, he says, marks a reevaluation of how enterprises handle data in order to quell employees' and customers' concerns and answer lingering questions after Snowden's revelations.

While a privacy officer might only focus on privacy-related endeavors, trust officers listen to both IT security professionals and the rest of the organization to ensure employees feel safe with a company having their data. They ensure employers have protections in place if data does become compromised, Thompson says.

Because data collection is well underway, organizations must focus on securing it and keeping its exposure to only relevant parties, says Darrin Reynolds, chief privacy officer (CPO) and VP of information security at Diversified Agency Services (DAS), a division of Omnicom Group, a New York-based global enterprise of marketing services and specialty communication companies.

“Instead of worrying about my information getting out, I would rather have stronger recourse for dealing with situations where information got misused for something I didn't like,” Reynolds says. “It won't be about control, but rather, consumer action on corporate accountability.”