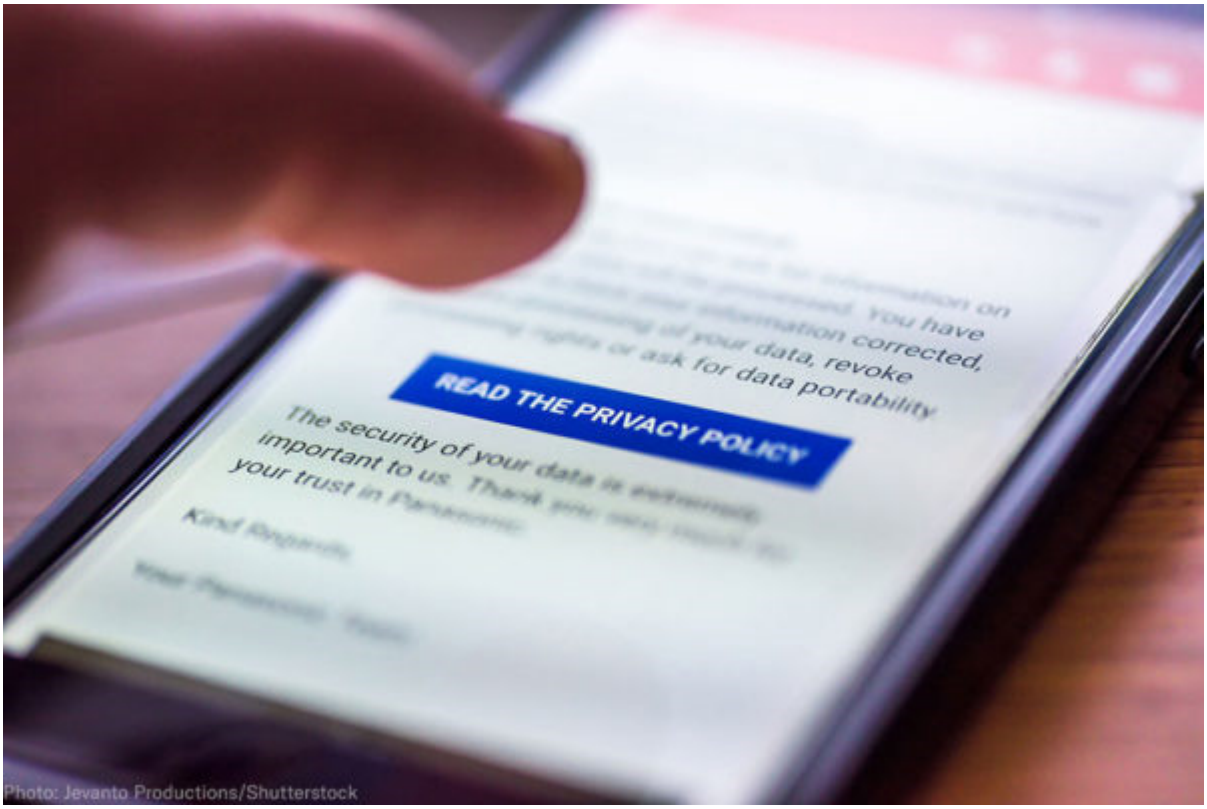
Three Common Privacy Misconceptions That Companies Love

Privacy-invading companies love it that people feel helpless, but now is the time for people to trade resignation for activism.



Jay Stanley , Senior Policy Analyst

November 14, 2019

A significant number of Americans hold significant misconceptions about their privacy, according to opinion research — misconceptions that privacy-invading companies love. That's according to research on American understandings of privacy carried out over the past couple decades by the Annenberg School for Communication at the University of Pennsylvania, lead by Prof. Joseph Turow, whom I recently heard give a talk summarizing these studies.

Misconception #1: "We care about your privacy!"

One misconception is that when a web site has a "privacy policy," that actually means the site has a policy to protect your privacy. Annenberg presented respondents with the false statement that "When a web site has a privacy policy, it means the site will not share my information with other websites or companies without my permission." In 2018, nearly 60 percent of Americans either said they believed this was true, or that they did not know. In past years the percentage of those surveyed giving incorrect answers was as high as 78 percent.

Unfortunately, nothing could be further from the truth. Most "privacy" polices start by declaring, "We care about your privacy!" and then go on to say, in extremely long and complicated legal language, that you have no privacy. Lawyers write these policies to minimize the presence of any actual concrete promises that might limit what a company does. Because the United States doesn't yet have a baseline privacy law, the only thing protecting our privacy in most commercial contexts is a prohibition on "acts or practices that are unfair or deceptive." That prohibition was enacted in 1914 — just *slightly* before the advent of today's online advertising surveillance systems. What that means is that (outside of a few narrow areas that are regulated such as credit reporting) a company can do whatever it wants with your personal information. The only thing it generally cannot do under federal law is *say* it's going to do one thing and then do another, which would count as "unfair or deceptive," and leave a company vulnerable to enforcement by the Federal Trade Commission.

Turow says that "marketers know" about this misconception and benefit from the confusion and the misplaced consumer trust it creates. Turow suggests that "privacy policy" is "a deceptive term" and that "the FTC should require a change in the label." "How We Use Your Data" would be more accurate.

Misconception #2: What is unfair is also illegal.

A second misconception that many Americans hold is that the law protects them more than it does. For example, in 2015, 62 percent of Americans didn't know that it is completely legal for an online store to "charge different prices to different people at the same time of day"; in 2012, 76 percent did not know that "online marketers are allowed to share information about diseases you or your family members have"; and in 2018, 46 percent did not know that an "internet provider has a legal right to sell information to marketers about the websites you visit." (We

think they actually *don't* have such a right under the Communications Act, which states that "every telecommunications carrier has a duty to protect the confidentiality" of personal information — but an attempt to craft detailed rules enforcing that law was killed by Congress and President Trump in 2017, and there's no sign that such a right will be enforced by the federal government anytime soon.)

What's going on here, Turow believes, is that people have fairly well-defined feelings about what kinds of behavior are fair and what are not — and they tend to think that things that are unfair are also illegal. They think, as he puts it, that the government has our backs much more than it actually does.

Annenberg's polling confirms other polling in consistently finding that people are deeply uncomfortable with the state of their privacy online. Two-thirds (66 percent) of adults, for example, told surveyors that they do not want advertisements "tailored to their interests," and 91 percent disagreed with the statement that "if companies give me a discount, it is a fair exchange for them to collect information about me without my knowing." Asked whether "It's okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me," 55 percent disagreed.

These findings, Turow concludes, "refute marketers' insistence that Americans find increased personalized surveillance and targeting for commercial purposes acceptable."

So why do people give up so much information? The problem is that they feel helpless. The surveys found that 58 percent of Americans agreed with the statement, "I want to have control over what marketers can learn about me online" — but at the same time 63 percent also agreed, "I've come to accept that I have little control over what marketers can learn about me online." Although marketers like to portray Americans as cheerfully accepting a tradeoff between their privacy and the benefits they gain, that's not at all what's happening. As Turow told me, "The bottom line for us is resignation. It's not as if people want to give up their privacy, but in order to get through life they feel they have to, and they don't feel like they have the ability to change things."

Misconception #3: We've lost the privacy battle.

This, I would argue, is the third misconception: that the battle is lost and there's nothing people can do about protecting their privacy. It's true that there are good reasons why people feel that way — there's only so much that an individual can do to protect their privacy, especially if they're short on technical expertise or willingness to tolerate inconveniences in order to fight surveillance. It's true that our privacy depends to a large extent not on individual decisions but on collective decisions we make as a nation about the policies we want to set. It's also true that the companies that profit from surveillance are wealthy and politically powerful.

Nevertheless, the clouds are gathering for a major reckoning. The European Union has enacted a comprehensive privacy law called the General Data Protection Regulation (GDPR) that is forcing even many U.S.-centered businesses to improve their privacy practices. California, where one in eight Americans live, has also enacted a broad privacy law called the California Consumer Privacy Act (CCPA). And as these laws weaken the will of companies to oppose privacy protections, scandals such as the Cambridge Analytica fiasco have strengthened the desire of politicians across the political spectrum to support such rules. The result: For the first time in many years, members of both parties are reportedly working to draft and enact comprehensive privacy legislation.

There are major battles ahead, but, as I have argued, in the end people need — and always demand — privacy. Privacy-invading companies love it that people feel helpless, but now is the time for people to trade resignation for anger and activism, and voice that demand to ensure that any new privacy laws are strong and meaningful. The status quo is not stable, and the battle is just getting underway.