Privacy Isn't Dead. Far From It.

Jason Kelley ⋮ 14-18 minutes ⋮ 2/13/2024

Welcome!

The fact that you're reading this means that you probably care deeply about the issue of privacy, which warms our hearts. Unfortunately, even though you care about privacy, or perhaps because you care so much about it, you may feel that there's not much you (or anyone) can really do to protect it, no matter how hard you try. Perhaps you think "privacy is dead."

We've all probably felt a little bit like you do at one time or another. At its worst, this feeling might be described as despair. Maybe it hits you because a new privacy law seems to be too little, too late. Or maybe you felt a kind of vertigo after reading a news story about a data breach or a company that was vacuuming up private data willy-nilly without consent.

People are angry because they care about privacy, *not* because privacy is dead.

Even if you don't have this feeling now, at some point you may have felt—or possibly will feel—that we're past the point of no return when it comes to protecting our private lives from digital snooping. There are so many dangers out there—invasive governments, doorbell cameras, license plate readers, greedy data brokers, mismanaged companies that haven't installed any security updates in a decade. The list goes on.

This feeling is sometimes called "privacy nihilism." Those of us who care the most about privacy are probably more likely to get it, because we know how tough the fight is.

We could go on about this feeling, because sometimes we at EFF have it, too. But the important thing to get across is that this feeling is valid, *but it's also not accurate*. Here's why.

You Aren't Fighting for Privacy Alone

For starters, remember that none of us are fighting alone. EFF is one of dozens, if not hundreds, of organizations that work to protect privacy. EFF alone has over thirty-thousand dues-paying members who support that fight—not to mention hundreds of thousands of supporters subscribed to our email lists and social media feeds. Millions of people read EFF's website each year, and tens of millions use the tools we've made, like Privacy Badger. Privacy is one of EFF's *biggest* concerns, and as an organization we have grown by leaps and bounds over the last two decades because *more and more people care*. Some people say that Americans have given up on privacy. But if you look at actual facts—not just EFF membership, but survey results and votes cast on ballot initiatives—Americans overwhelmingly support new privacy protections. In general, the country has grown more concerned about how the government uses our data, and a large majority of people say that we need more data privacy protections.

People are angry because they care about privacy, *not* because privacy is dead.

Some people also say that kids these days don't care about their privacy, but the ones that we've met think about privacy a lot. What's more, they are fighting as hard as anyone to stop privacy-invasive bills like the Kids Online Safety Act. In our experience, the next generation cares intensely about protecting privacy, and they're likely to have even more tools to do so.

Laws are Making Their Way Around the World

Strong privacy laws don't cover every American—yet. But take a look at just one example to see how things are improving: the California Consumer Privacy Act of 2018 (CCPA). The CCPA isn't perfect, but it did make a difference. The CCPA granted Californians a few basic rights when it comes to their relationship with businesses, like the right to know what information companies have about you, the right to delete that information, and the right to tell companies not to sell your information.

This wasn't a perfect law for a few reasons. Under the CCPA, consumers have to go company-by-company to opt out in order to protect their data. At EFF, we'd like to see privacy and protection as the default until consumers opt-*in*. Also, CCPA doesn't allow individuals to sue if their data is mismanaged—only California's Attorney General and the California Privacy Protection Agency can do it. And of course, the law only covers Californians.

Remember that it takes time to change the system.

But this imperfect law is slowly getting better. Just this year California's legislature passed the DELETE Act, which resolves one of those issues. The California Privacy Protection Agency now must create a deletion mechanism for data brokers that allows people to make their requests to every data broker with a single, verifiable consumer request.

Pick a privacy-related topic, and chances are good that model bills *are* being introduced, or already exist as laws in some places, even if they don't exist everywhere. The Illinois Biometric Information Privacy Act, for example, passed back in 2008, protects people from nonconsensual use of their biometrics for face recognition. We may not have comprehensive privacy laws yet in the US, but other parts of the world—like Europe—have more impactful, if imperfect, laws. We *can* have a nationwide comprehensive consumer data privacy law, and once those laws are on the books, they can be improved.

We Know We're Playing the Long Game

Remember that it takes time to change the system. Today we take many protections for granted, and often assume that things are only getting worse, not better. But many important rights are relatively new. For example, our Constitution didn't always require police to get a warrant before wiretapping our phones. It took the Supreme Court four decades to get this right. (They were wrong in 1928 in *Olmstead*, then right in 1967 in *Katz*.)

Similarly, creating privacy protections in law and in technology is not a sprint. It is a marathon. The fight is long, and we know that. Below, we've got examples of the progress that we've already made, in law and elsewhere.

Just because we don't have some protective laws today doesn't mean we can't have them tomorrow.

Privacy Protections Have Actually Increased Over the Years

The World Wide Web is Now Encrypted

When the World Wide Web was created, *most* websites were unencrypted. Privacy laws aren't the only way to create privacy protections, as the now nearly-entirely encrypted web shows: another approach is to engineer in strong privacy protections from the start.

The web has now largely switched from non-secure HTTP to the more secure HTTPS protocol. Before this happened, most web browsing was vulnerable to eavesdropping and content hijacking. HTTPS fixes most of these problems. That's why EFF, and many like-minded supporters, pushed for web sites to adopt HTTPS by default. As of 2021, about 90% of all web page visits use HTTPS. This switch happened in under a decade. This is a big win for encryption and security for everyone, and EFF's Certbot and HTTPS Everywhere are tools that made it happen, by offering an easy and free way to switch an existing HTTP site to HTTPS. (With a lot of help from Let's Encrypt, started in 2013 by a group of determined researchers and technologists from EFF and the University of Michigan.) Today, it's the default to implement HTTPS.

Cell Phone Location Data Now Requires a Warrant

In 2018, the Supreme Court handed down a landmark opinion in *Carpenter v. United States*, ruling 5-4 that the Fourth Amendment protects cell phone location information. As a result, police must now get a warrant before obtaining this data.

But where else this ruling applies is still being worked out. Perhaps the most significant part of the ruling is its explicit recognition that individuals can maintain an expectation of privacy in information that they provide to third parties. The Court termed that a "rare" case, but it's clear that other invasive surveillance technologies, particularly those that can track individuals through physical space, are now ripe for challenge. Expect to see much more litigation on this subject from EFF and our friends.

Americans' Outrage At Unconstitutional Mass Surveillance Made A Difference

In 2013, government contractor Edward Snowden shared evidence confirming, among other things, that the United States government had been conducting mass surveillance on a global scale, including surveillance of its own citizens' telephone and internet use. Ten years later, there is definitely more work to be done regarding mass surveillance. But some things are undoubtedly better: some of the National Security Agency's most egregiously illegal programs and authorities have shuttered or been forced to end. The Intelligence Community has started affirmatively releasing at least some important information, although EFF and others have still had to fight some long Freedom of Information Act (FOIA) battles.

Privacy Options Are So Much Better Today

Remember PGP and GPG? If you do, you know that generally, there are much easier ways to send end-to-end encrypted communications today than there used to be. It's fantastic that people worked so hard to protect their privacy in the past, and it's fantastic that they don't have to work as hard now! (If you aren't familiar with PGP or GPG, just trust us on this one.)

Don't give in to privacy nihilism. Instead, share and celebrate the ways we're winning.

Advice for protecting online privacy used to require epic how-to guides for complex tools; now, advice is usually just about what relatively simple tools or settings to use. People across the world have Signal and WhatsApp. The web is encrypted, and the Tor Browser lets people visit websites anonymously fairly easily. Password managers protect your passwords and your accounts; third-party cookie blockers like EFF's Privacy Badger stop third-party tracking. There are even options now to turn off your Ad ID—the key that enables most third-party tracking on mobile devices—right on your phone. These tools and settings all push the needle forward.

We Are Winning The Privacy War, Not Losing It

Sometimes people respond to privacy dangers by comparing them to sci-fi dystopias. But be honest: most science fiction dystopias still scare the heck out of us because they are *much, much* more invasive of privacy than the world we live in.

In an essay called "Stop Saying Privacy Is Dead," Evan Selinger makes a necessary point: "As long as you have some meaningful say over when you are watched and can exert agency over how your data is processed, you will have some modicum of privacy."

Of course we want more than a modicum of privacy. But the point here is that many of us generally *do* get to make decisions about our privacy. Not all—of course. But we all recognize that there are different levels of privacy in different places, and that privacy protections aren't equally good or bad no matter where we go. We have places we can go—online and off—that afford us more protections than others. And because of this, most of the people reading this still have deep private lives, and can choose, with varying amounts of effort, not to allow corporate or government surveillance into those lives.

Worrying about every potential threat, and trying to protect yourself from each of them, all of the time, is a recipe for failure.

Privacy is a process, not a single thing. We are always negotiating what levels of privacy we have. We might not always have the upper hand, but we are often able to negotiate. This is why we still see some fictional dystopias and think, "Thank God that's not my life." As long as we can do this, we are winning.

"Giving Up" On Privacy May Not Mean Much to You, But It Does to Many

Shrugging about the dangers of surveillance can seem reasonable when that surveillance isn't very impactful on our lives. But for many, fighting for privacy isn't a choice, it is a means to survive. Privacy inequity is real; increasingly, money buys additional privacy protections. And if privacy is available for some, then it can exist for all. But we should not accept that some people will have privacy and others will not. This is why digital privacy legislation is digital rights legislation, and why EFF is opposed to data dividends and pay-for-privacy schemes.

Privacy increases for all of us when it increases for each of us. It is much easier for a repressive government to ban end-to-end encrypted messengers when only journalists and activists use them. It is easier to know who is an activist or a journalist when they are the only ones using privacy-protecting services or methods. As the

number of people demanding privacy increases, the safer we all are. Sacrificing others because you don't feel the impact of surveillance is a fool's bargain.

Time Heals Most Privacy Wounds

You may want to tell yourself: companies already know everything about me, so a privacy law a year from now won't help. That's incorrect, because companies are always searching for new data. Some pieces of information will never change, like our biometrics. But chances are you've changed in many ways over the years—whether that's as big as a major life event or as small as a change in your tastes in movies—but who you are today is not necessarily you'll be tomorrow.

As the source of that data, we should have more control over where it goes, and we're slowly getting it. But that expiration date means that even if some of our information is already out there, it's never going to be too late to shut off the faucet. So if we pass a privacy law next year, it's not the case that every bit of information about you has already leaked, so it won't do any good. It will.

What To Do When You Feel Like It's Impossible

It can feel overwhelming to care about something that feels like it's dying a death of a thousand cuts. But worrying about every potential threat, and trying to protect yourself from each of them, all of the time, is a recipe for failure. No one really needs to be vigilant about every threat at all times. That's why our recommendation is to create a personalized security plan, rather than throwing your hands up or cowering in a corner.

Once you've figured out what threats you should worry about, our advice is to stay involved. We are all occasionally skeptical that we can succeed, but taking action is a great way to get rid of that gnawing feeling that there's nothing to be done. EFF regularly launches new projects that we hope will help you fight privacy nihilism. We're in court many times a year fighting privacy violations. We create ways for like-minded, privacy-focused people to work together in their local advocacy groups, through the Electronic Frontier Alliance, our grassroots network of community and campus organizations fighting for digital rights. We even help you teach others to protect their own privacy. And of course every day is a good day for you to join us in telling government officials and companies that privacy matters.

We know we can win because we're creating the better future that we want to see every day, and it's working. But we're also building the plane while we're flying it. Just as the death of privacy is not inevitable, neither is our success. It takes real work, and we hope you'll help us do that work by joining us. Take action. Tell a friend. Download Privacy Badger. Become an EFF member. Gift an EFF membership to someone else.

Don't give in to privacy nihilism. Instead, share and celebrate the ways we're winning.