The WIRED Guide to Protecting Yourself From Government Surveillance

Andy Greenberg, Lily Hay Newman ⋮ 22-27 minutes ⋮ 11/12/2024

President-elect Donald Trump has promised to deport millions of undocumented immigrants. He's vowed to jail his political foes and journalists. A Republican-controlled government could further restrict abortion and transgender rights. Influential conservatives have called for a crackdown on left-leaning activist groups, a replay of Trump's hardline attitude against protesters in his first administration.

To carry out all of those spoken and unspoken threats, the incoming Trump administration and Republicans in Congress will tap into—and may very well expand—the American government's vast surveillance machinery, and they appear poised to use it more than any administration in recent US history.

That means now is the time for anyone in an at-risk group, those who communicate with them—or even those who want to normalize privacy and create cover for more vulnerable people—to think about how they can upgrade their data security and surveillance resistance ahead of a second Trump administration.

“Undocumented immigrants, Muslims, pregnant people, journalists, really anyone who doesn't support him” need to reconsider their personal privacy safeguards, says Runa Sandvik, a former digital security staffer for The New York Times and the founder of the security firm Granitt, which focuses on protecting members of civil society. “Whatever platforms you're on, whatever devices you have, you need to have a sense of what kind of data you're generating and then use the controls available to limit who can see what you're doing.”

Protection from surveillance comes in two forms: top-down legal and policy limits on data collection, and bottom-up technological protections in the hands of the targets of that surveillance. A new era looms just weeks ahead where Trump and his allies control all three branches of government and tech companies will very likely bend to their will—as evidenced by the Silicon Valley CEOs' race to congratulate the president-elect.

That may leave the technology you choose to use as a last line of defense, says Harlo Holmes, the director of digital security at the Freedom of the Press Foundation. “This is the last recourse of a lot of people in vulnerable positions,” says Holmes. “We're just going to have to increase our efforts to make sure that people have the best tools in their hands and their pockets to maintain their privacy. And it's going to matter more and more.”

Ahead of that impending new reality, WIRED asked security and privacy experts for their advice for hardening personal privacy protections and resisting surveillance. Here are their recommendations.

Encrypted Communications

Securing your data starts with securing your communications, and securing your communications means using end-to-end encryption.

End-to-end encrypted messengers like Signal, WhatsApp, and Apple's iMessage and FaceTime are all designed to encrypt your messages and phone calls such that no one can decrypt and access your conversations other than the recipient—not even the company that offers the service. That's very different from traditional calls and texts, which are subject to law enforcement interception and data requests to your phone carrier.

Digital services like Facebook Messenger, Telegram, or X may say their direct messages offer "encryption," but in the default setting that almost everyone uses, they only encrypt information in transit to the server that runs the service. On that server, the information is then decrypted and accessible to the company that controls that server, or any government agency that demands they share that data—like the Nebraska police who demanded Facebook hand over chats about a 17-year-old's illegal abortion in 2022, then brought criminal charges against her and her mother.

Among actual end-to-end encrypted messengers, Signal is broadly recommended as offering the best privacy protections. Importantly, Signal doesn't collect or store metadata about who is calling or texting whom, information that can often be nearly as sensitive as the content of conversations. That's a crucial safeguard given that Trump has said in his recent campaigning, for instance, that he will hunt down and prosecute government staffers leaking information to journalists—and his previous administration seized the phone and email records of reporters at The New York Times and CNN. With Signal, there are no records to seize. "Metadata matters," says Holmes.

Just as important is that Signal offers flexible settings for "disappearing messages" that self-delete on every device used in a conversation after a chosen time, in as little as five seconds. Be sure to turn this feature on to prevent messages from being read in the event that your phone is seized—or the phone of the person on the other side of the conversation. Signal also doesn't back up communication logs to iCloud or other cloud services, so there's less risk that a participant in the conversation will accidentally leak everyone's messages to a server where they can be accessed. "If it's up to me, I will choose Signal, because I know that there is less that you can do on *your* end to potentially put our communications at risk," says Granitt's Sandvik.

Encrypted Devices

Just as important as encrypting your conversations is strongly encrypting your devices themselves.

On modern iOS and Android smartphones, that's relatively easy. They're designed to use full disk encryption by default: All the data is encrypted when they're locked. That means setting a six-digit passcode is enough to make cracking the device a serious challenge, given that both Android and iOS limit the number of times someone can guess a passcode before the device is wiped as a security measure. Still, the Freedom of the Press Foundation's Holmes recommends setting a longer alphanumeric password or passphrase on your phone to make it harder still to break into. (On an iPhone, go to "Settings," "FaceID & Passcode," "Change Passcode," "Passcode Options," re-enter your passcode and then choose "Custom Alphanumeric Code." On Android, the path to change the setting varies by device.)

Entering a 34-character passphrase every time you want to unlock your phone is, admittedly, a nightmare. So Holmes recommends also using the biometric features built into smartphones like Apple's FaceID. That does present the risk that someone who grabs your phone will exploit this feature: You can tell a police officer or FBI agent you forgot your iPhone's passcode, like indicted New York mayor Eric Adams did, but you can't remove your face. You can, however, temporarily disable biometric unlocking features with a long press on an Android phone's power button or by holding the side button and one volume button on an iPhone, so that the next unlock requires the passcode.

"Let's say you're protesting, or if you're going through a border crossing," says Holmes. "There's always that gesture that clears your biometrics." She recommends practicing that trick before going into a setting where you might need to use it.

Encrypting a laptop requires slightly more effort. On a Macbook, enable Apple's built-in FileVault's full disk encryption in your computer's privacy and security settings. On Windows, use the built-in Bitlocker encryption setting if you have a Windows Pro license. If you have a Home license, install and enable an encryption tool called Veracrypt.

For both smartphones and laptops, keep in mind that cracking a device's encryption is far more difficult when it's been powered off, which prevents the cryptographic keys that unlock the device from lingering in memory. So it's always a good idea—for security's sake—to switch off your computer and phone when they're not in use or you're entering a situation where they might be seized.

Cloud Storage

Whether it's extra storage for all of your photos and videos or merely your contacts and messages syncing between your phone and your tablet, you're almost inevitably using cloud services to back up and sync your information. When your data lives on the hard drive of your computer or smartphone, it's stored "locally" and you control it. Before the rise of the internet, this local, decentralized storage model was the norm. Companies had their data on their own servers, and regular people had their data on their home computers. Today, though, you can save your data—from documents to phone backups—in your own little corner of the cloud and let tech giants like Amazon, Google, Microsoft, and Apple manage the storage infrastructure for you. Web services, whether they are social networks or your go-to cooking app, similarly store your account data in the cloud so you can access your favorite recipes and all of your annotations from any device with an internet connection.

Cloud storage has huge advantages—you never run out of hard drive space, and your data won't be lost forever when an ill-fated Diet Coke spills on your laptop. The trade-off, though, is that storing data in the cloud adds a third party to the mix. Cloud companies that hold and manage your data can almost always access it, which means they can be compelled to hand it over to governments. US law enforcement gathered evidence about now-convicted former Trump campaign chair Paul Manaforte in part by accessing unencrypted iCloud backups of his WhatsApp chat histories. And in 2020, the FBI got access to a protester's iCloud account from Apple—including photos, videos, and screenshots—over accusations that he lit police cars on fire in Seattle.

In recent years, more companies have begun offering end-to-end encrypted data backups and storage schemes for their cloud services so customers can use cloud infrastructure without worrying that the provider can access their data—and potentially give it away. Apple's iCloud backups and backups for Meta's chat apps, Facebook Messenger, Instagram Chat, and WhatsApp, can all be encrypted now. But to benefit from the protection you need to make sure that you actually have the feature turned on. And from there you have to set up mechanisms to preserve your access to the data and be able to recover your account if you're ever locked out, since end-to-end encryption schemes mean that you no longer have the convenience of the cloud provider managing access.

In general, privacy advocates agree that the simplest way to ensure that data doesn't fall into the wrong hands is to keep it out of the cloud in the first place. Each time you use a different device or digital account, think for a second about whether your data is stored on your device or in the cloud. And if you realize it's the latter, consider whether you trust the service provider to store that data for you.

For example, as Holmes puts it, "Take a moment to make sure that the things that you are deliberately syncing to your iCloud are the things that you wouldn't mind someone having access to."

If you really need to store private data in the cloud, you can use a tool like Veracrypt to encrypt the information before uploading it. But the easiest and safest option is to keep anything particularly sensitive or revealing out of the cloud.

Online Anonymity

Your communications and the data on your devices are far from the only sensitive digital records you're constantly creating. You're also leaving behind a trail of breadcrumbs on the paths you take around the internet—paths that are all too visible to your internet service provider and the websites you visit, and which can be highly revealing to anyone building a profile of you and your behavior.

"For me, I always say it's important to remember you're not 'going to' a website," says Matt Mitchell, founder of CryptoHarlem, a security and privacy training and advocacy nonprofit. "You're opening a door, and just like if you open your door, people can see you, and they can see behind you."

The strongest tool available to obscure your trail online is the Tor Browser. That browser for desktops and laptops, or the mobile equivalent called Orbot, both offered by the nonprofit Tor Project, triple-encrypt your web-browsing data and bounce your connection to the sites you visit through a series of proxy computers. Each of those proxy machines can only decrypt one of those three layers of encryption so that none of the machines can determine the full path of your connection or tie the internet protocol address that would reveal your identity and location to the sites you're visiting. Your IP address is also hidden from the website itself.

Tor's encrypted triple-proxy system can, however, be slow, and some websites are configured to block connections from the Tor network or force users to fill out annoying captchas. So the Freedom of the Press Foundation's Holmes suggests users try the private browsing feature in the Brave browser, which uses a stripped-down version of Tor's anonymous routing by default. Apple also offers a feature called iCloud Private Relay, which uses a two-hop proxy system rather than Tor's three-hop system to obscure your web browsing, which may well be faster and more convenient, but it requires a paid monthly subscription to the company's iCloud+ services.

In addition to using a privacy-focused browser, one of the most practical tools for the majority of users is a virtual private network or VPN—essentially a service that offers a one-hop version of Tor's privacy protections. Many commercial VPNs do log users' browsing and respond to law enforcement requests for that data, however, so choosing a VPN with strong privacy guarantees for its users can be a challenge. Holmes suggests referring to the Freedom of the Press Foundation's VPN guide.

For those who can't or don't want to use Tor-based tools, a carefully chosen VPN remains a powerful form of protection. "Having a VPN in your pocket that doesn't do any logging at all of your activity and also provides robust controls is the next best thing," Harlo Holmes says.

Location Data

One of the most difficult—and crucial—types of personal information to get a handle on is your location data. Any entity that can track your location or obtain records of where you've gone can gain a full picture of where you live and work, who you know and care about, which businesses and medical services you use, and even what you believe in or the causes you support.

Protecting information about your movements is critical to your own privacy and security under expanding government surveillance and is significant in protecting the privacy of those you associate with.

Danacea Vo, founder of Cyberlixir, a cybersecurity provider for nonprofits and vulnerable communities, says that societal changes like the loss of federal abortion protections in the United States, are a reality check about the shifting digital privacy landscape and "help people realize how important it is to hide their location data, because something that might be completely legal today might not be legal tomorrow."

Your smartphone is essentially a tracking beacon that you carry with you all the time. And it's important to remember that other devices like laptops, not to mention literal tracking beacons like AirTags and Tiles, can also reveal your movements.

You can limit the location tracking that your mobile apps and mobile operating system are automatically doing to cut down on the number of companies and other entities that have the information. On both iOS and Android you can manage which apps and operating system services have access to the information and when. Turn off location access for as many apps as possible and regularly review and delete apps you don't use anymore. You can also take similar precautions on desktop. And make sure that overarching accounts like your Google or Apple ID/iCloud accounts haven't logged trusted places like a "home" for you.

Turning on a VPN, using a privacy-focused mobile browser, and adding an ad blocker can all help reduce the location data you leak during mobile browsing. iPhone users can also gain location-protecting features by turning on Apple's Lockdown Mode, which is meant to minimize the ways that someone can attack your device—particularly limiting features that could be exploited by hackers to plant spyware. Lockdown Mode provides extra protections relevant to location privacy, like removing location metadata from photos when you go to share them and stopping your device from auto-joining public or otherwise unprotected Wi-Fi networks. But using Lockdown Mode significantly restricts your iPhone’s features. Unless you believe that you are under specific threat of targeted surveillance or digital attack, it isn’t the most practical tool for daily life.

No matter how much you’ve limited location tracking in apps and operating systems, your smartphone can also be tracked through your cellular service because your device pings cell towers around you to stay connected to the network. That’s why the easiest way to be certain that your devices aren’t collecting or leaking your whereabouts is to not carry them. If you don’t create the data in the first place, no one can access it.

“If you’re trying to not be tracked, not having a phone is often the easiest,” Sandvik says. “Leave it at home.”

For most people most of the time, though, this solution isn’t practical. You can put your devices in airplane mode or turn them off completely to limit connectivity. But to be totally certain that everything is off the grid, you can put your devices in special pouches or cases known as Faraday bags that block all electromagnetic signals going to or coming from a device. Faraday bags allow you to carry your devices while keeping them from exposing your location; for example, concealing your whereabouts on a given afternoon or the route you took to get to a destination. The downside of Faraday bags is the device must stay in the bag to protect your privacy, so it takes planning to use them effectively. Removing your phone means that the (location) cat is out of the bag.

Financial Privacy

Financial surveillance is among the most powerful tracking tools in the government’s arsenal. Credit card payments or other transactions linked to your bank account are essentially transparent to any law enforcement agency that demands them.

That “follow the money” form of surveillance also has a relatively simple analog defense: dollar bills. “Forensic accounting is a thing,” warns Holmes. “So yeah, use cash.”

For those seeking more convenient or long-distance transactions, payment apps like Paypal, Venmo, and Cash App may seem slightly more cash-like than a credit card or check, but in fact are just as vulnerable to law enforcement data requests as any bank. Cryptocurrency may appear to be a tempting alternative. But despite the long-running mythical reputation of cryptocurrency as anonymous cash for the internet, bitcoin and most other cryptocurrencies offer no real privacy, given the ease of tracing bitcoin transactions on its blockchain and the difficulty of buying or selling cryptocurrency from a cryptocurrency exchange that complies with US know-your-customer laws.

Some cryptocurrencies like Monero and Zcash do offer privacy properties that make them vastly more difficult to trace than other cryptocurrencies—at least in theory. Mixer services like the Ethereum-based Tornado Cash, too, promise to blend users’ coins with those of others to complicate the task of following the money. Still, given the ongoing advances in cryptocurrency tracing—and the indelible evidence of any security slipup that public blockchains make available to the cats in that cat-and-mouse game—it’s far safer to stick with cash whenever possible.

A Note on Burner Phones

Burner phones, or prepaid phones that aren't connected to any of your credit cards or digital accounts, can be a useful tool for protecting your location data and other information. They are meant to have no traceable connection to you and to be used for a limited time. In other words, they are meant to provide anonymity.

The advantage to using burner devices is that you don't need to worry as much about the personal information they are collecting or inadvertently leaking while you use them because the devices are not linked to you. They merely show that someone is going here and there or that someone has, say, planned to meet someone else at 8 pm on the park benches. Over time, though, if you, use the device to communicate often, log into any digital accounts that are associated with you from the device, give a burner number to people who don't use burners themselves, or bring it to a location associated with you while it's on, like your house, the phone could quickly be linked to you.

On top of all of these restrictions, burner phones should always be acquired with cash. But even when people take this precaution, it can still be difficult in practice to purchase a burner device without leaving a trail of potentially identifying clues.

For all of these reasons, many privacy advocates do not recommend burner phones for the majority of people. Holmes suggests that people instead "compartmentalize" and control their data by having a second phone that separates some activities, like work versus personal life. This way, you don't accidentally end up with photos of your family in your work's cloud storage, say, or with confidential information from work on your personal device.

"Unless you're gonna pretend to be a character from *The Wir*e, ultimately what's attainable for people is compartmentalization, not anonymity," Holmes says.

Your Digital Past, Present, and Future

If you've made it this far, you know that there are real, concrete steps you can take to resist surveillance and defend your digital privacy in everyday life. But for even the most dedicated digital hermits, there are limits to how much you can control.

At this point, information about almost everyone—whether it's basic personal information, health data, or financial records—has likely been compromised at some point in at least one big data breach. This means that no matter how careful you've been, some details about you are likely available to anyone who wants to dig them up, either legally or through the cybercriminal ecosystem. If your privacy practices have been less than perfect in the past—and whose have not, given the vanishingly tiny odds of evading every form of digital data collection—additional information about you from over the years is likely available from hundreds of data brokers. These companies give anyone who will pay—including governments—access to vast troves of advertising and marketing information, which can often include location data.

That means any reader of this guide should be aware that, careful as they may be now or in the future, digital evidence from their past can still be dug up and used to track or target them. “You can make changes today and moving forward, but there's likely a lot of data that's already available that can be abused,” warns Sandvik.

Still, it’s better to start somewhere than never to start at all. Even if you haven’t tried to protect your digital privacy in the past, your future self may be in a situation, someday, where you appreciate that you started taking precautions now. With a new Trump administration weeks away from inauguration—a government openly committed to targeting its enemies with every tool available and hunting many of the country’s most vulnerable people—that someday may be sooner than you think.