How to Protest Safely in the Age of Surveillance

Andy Greenberg, Lily Hay Newman

Just days into 2026, fresh anger against the Trump administration has already taken hold.

On Wednesday, January 7, a federal immigration officer shot and killed 37-year-old Renee Nicole Good as she attempted to drive away from the scene of an immigration enforcement action in a Minneapolis, Minnesota, neighborhood. Despite Department of Homeland Security secretary Kristi Noem's claims that the officer “acted quickly and defensively, shot, to protect himself and the people around him” from being run over, video of the incident clearly appears to show that neither the officer nor his colleagues were in danger of being hit by Good's vehicle.

Protests condemning the shooting—and the Trump administration's brutish immigration agenda more broadly—sparked almost immediately after news of Good's killing surfaced. By Thursday, the unrest had only intensified and spread to towns and cities around the United States.

If you're going to join any protests, as is your right under the First Amendment, you need to think beyond your physical well-being to your digital security, too. The same surveillance apparatus that’s enabling the Trump administration’s raids of undocumented people and targeting of left-leaning activists will no doubt be out in full force on the streets.

Two key elements of digital surveillance should be top of mind for protestors. One is the data that authorities could potentially obtain from your phone if you are detained, arrested, or they confiscate your device. The other is surveillance of all the identifying and revealing information that you produce when you attend a protest, which can include wireless interception of text messages and more, and tracking tools like license plate scanners and face recognition. You should be mindful of both.

After all, even before Good's killing, police had already demonstrated their willingness to arrest and attack entirely peaceful protesters as well as journalists observing demonstrations. In that light, you should assume that any digital evidence that you were at or near a protest could be used against you.

“The Trump administration is weaponizing essentially every lever of government to shut down, suppress, and curtail criticism of the administration and of the US government generally, and there have never been more surveillance toys available to law enforcement and to US government agencies,” says Evan Greer, the deputy director of the activist organization Fight for the Future, who also wrote a helpful X (then-Twitter) thread laying out digital security advice during the Black Lives Matter protests in the summer of 2020. “That said, there are a number of very simple, concrete things that you can do that make it exponentially more difficult for someone to intercept your communications, for a bad actor to ascertain your real-time location, or for the government to gain access to your private information.”

This story was originally published on May 31, 2020 and updated on January 8, 2026.

Your Phone

The most important decision to make before leaving home for a protest is whether to bring your phone—or what phone to bring. A smartphone broadcasts all sorts of identifying information; law enforcement can force your mobile carrier to cough up data about what cell towers your phone connects to and when. Police in the US have also been documented using so-called stingray devices, or IMSI catchers, that impersonate cell towers and trick all the phones in a certain area into connecting to them. This can give cops the individual mobile subscriber identity number of everyone at a protest at a given time,

undermining the anonymity of entire crowds en masse.

“The device in your pocket is definitely going to give off information that could be used to identify you,” says Harlo Holmes, director of digital security at the Freedom of the Press Foundation, a nonprofit press advocacy group. (Disclosure: WIRED’s global editorial director, Katie Drummond, serves on Freedom of the Press Foundation’s board.)

For that reason, Holmes suggests that protesters who want anonymity leave their primary phone at home altogether. If you do need a phone for coordination or as a way to call friends or a lawyer in case of an emergency, keep it off as much as possible to reduce the chances that it connects to a rogue cell tower or Wi-Fi hot spot being used by law enforcement for surveillance. Sort out logistics with friends in advance so you only need to turn your phone on if something goes awry. Or to be even more certain that your phone won’t be tracked, keep it in a Faraday bag that blocks all of its radio communications. Open the bag only when necessary. Holmes herself uses and recommends the Mission Darkness Faraday bag.

If you do need a mobile device, consider bringing only a secondary phone you don’t use often, or a burner. Your main smartphone likely has the majority of your digital accounts and data on it, all of which law enforcement could conceivably access if they confiscate your phone. But don’t assume that any backup phone you buy will grant you anonymity. If you give a prepaid carrier your identifying details, after all, your “burner” phone could be no more anonymous than your primary device. “Don’t expect because you got it from Duane Reade that you’re automatically a character from *The Wire*,” Holmes cautions.

Since properly using a burner phone can be impractical at best, Holmes says you may be better off using a secondary phone that excludes things like social media, email, and messaging apps. These apps and accounts can contain highly private information that could be exposed to anyone who seizes it. “Choosing a secondary device that limits the amount of personal data that you have on you at all times is probably your best protection,” Holmes says.

Regardless of what phone you’re using, consider that traditional calls and text messages are vulnerable to surveillance. That means you need to use end-to-end encryption. Ideally, you and those you communicate with should use disappearing messages set to self-delete after a few hours or days. The encrypted messaging and calling app Signal has perhaps the best and longest track record. Just make sure you and the people you’re communicating with are using the same app, since they’re not interoperable.

Aside from protecting your phone’s communications from surveillance, be prepared in the event police seize your device and try to unlock it in search of incriminating evidence. The first order of business is to make sure your smartphone’s contents are encrypted. iOS devices have full disk encryption on by default if you enable an access lock. For Android phones, go to **Settings**, then **Security** to make sure the **Encrypt Disk** option is turned on. (These steps may differ depending on your specific device.)

Regardless of your operating system, always protect devices with a long, strong passcode rather than a fingerprint or face unlock. As convenient as biometric unlocking methods are, it may be more difficult to resist an officer forcing your thumb onto your phone’s sensor, for instance, than to refuse to tell them a passcode. So if you use biometrics day-to-day for convenience, disable them before heading into a protest.

-
-
-
-
-

If you insist on using biometric unlocking methods to have faster access to your devices, keep in mind that some phones have an emergency function to disable these types of locks. Hold the wake button and one of the volume buttons simultaneously on an iPhone, for instance, and it will lock itself and require a passcode to unlock rather than FaceID or TouchID, even if they're enabled. Most devices also let you take photos or record video without unlocking them first, a good way to keep your phone locked as much as possible.

Your Face

Face recognition has become one of the most powerful tools to identify your presence at a protest. Consider wearing a face mask and sunglasses to make it far more difficult for you to be identified by face recognition in surveillance footage or social media photos or videos of the protest. Fight for the Future's Greer cautions, however, that the accuracy of the most effective face recognition tools available to law enforcement remains something of an unknown, and a simple surgical mask or KN95 may no longer be enough to defeat well-honed face-tracking tech.

If you're serious about not being identified, she says, a full-face mask may be far safer—or even a Halloween-style one. "I've seen people wear funny cosplay-style cartoon masks or mascot suits or silly costumes," says Greer, offering as an example Donald Trump and Elon Musk masks that she's seen protesters wear at Tesla Takedown protests against Musk and the so-called Department of Government

Efficiency (DOGE). “That's a great way to defy facial recognition and also make the protest more fun.”

You should also consider the clothes you’re wearing before you head out. Colorful clothing or prominent logos makes you more recognizable to law enforcement and easier to track. If you have tattoos that make you identifiable, consider covering them.

Greer cautions, though, that preventing determined surveillance-empowered agencies from learning the mere fact that you attended a protest at all is increasingly difficult. For those of you in the most sensitive positions—such as undocumented immigrants at risk of deportation—she suggests that you consider staying home rather than depend on any obfuscation technique to mask their presence at an event.

Another factor to weigh is your mode of transportation. Driving a car to a protest—whether it's yours or someone else's—can expose you to surveillance from automatic license plate readers, or ALPRs, which can be used to pinpoint a vehicle’s movements. You should also be aware that, in addition to license plates, these ALPRs can detect other words and phrases, including those on bumper stickers, signs, and even T-shirts.

More broadly, everyone who attends a protest needs to consider—perhaps more than ever before—what their tolerance for risk might be, from mere identification to the possibility of arrest or detention. “I think it's important to say that protesting in the US now comes with higher risks than it used to—it comes with a real possibility of physical violence and mass arrest,” says Danacea Vo, the founder of Cyberlixir, a cybersecurity provider for nonprofits and vulnerable communities. “Even just compared to protests that happened last month, people were able to just show up barefaced and march. Now things have changed.”

Your Online Footprint

Though most privacy and security considerations for attending an in-person protest naturally relate to your body, any devices you bring with you, and your physical surroundings, there are a set of other factors to think about online. It’s important to understand how posts on social media and other platforms before, during, or after a protest could be collected and used by authorities to identify and track you or others. Simply saying on an online platform that you are attending or attended a protest puts the information out there. And if you take photos or videos during a protest, that content could be used to expand law enforcement’s view of who attended a protest and what they did while there, including any strangers who appear in your images or footage.

Authorities can come to your online presence by looking for information about you in particular, but can also arrive there using bulk data analysis tools like Dataminr that offer law enforcement and other customers real-time monitoring connecting people to their online activity. Such tools can also surface past posts, and if you’ve ever made violent comments online or alluded to committing crimes—even as a joke—law enforcement could discover the activity and use it against you if you are questioned or arrested during a protest. This is a particular concern for people living in the US on visas or those whose immigration status is tenuous. The US State Department has said explicitly that it is monitoring immigrants’ and travelers’ social media activity.

In addition to written posts, keep in mind that files you upload to social media might contain metadata like time stamps and location information that could help authorities track protest crowds and movement. Make sure you have permission to photograph or videotape any fellow protesters who would be

potentially identifiable in your content. Also think carefully before livestreaming. It's important to document what's going on but difficult to be sure that everyone who could show up in your stream is comfortable being included.

Even if you take photos and videos that you don't plan to post on social media or otherwise share, remember that this media could fall into law enforcement's hands if they demand access to your device.

With the Trump administration ramping up its attempts to target and punish left-leaning people and organizations, Cyberlixir's Vo argues that people must assess the risks of every demonstration or other situation and judge for themselves the benefits of maintaining their personal privacy against the need to document the actions of government agents.

"Social media monitoring and online profiling is the factor that lots of people forget. Those who publish footage on social media should avoid sharing photos or videos that reveal people's faces," she says. "But I also believe that documenting what's going on is essential, especially in high-risk conditions, because when the state escalates we need proof for legal defense, for public record, for future organizing, and also to keep ourselves physically safe in real time."

As protests continue—with the real possibility of even further escalated response from the Trump administration—be prepared for the emergence of forms of digital surveillance that have never been used in the US before to counter civil disobedience or to retaliate against protesters after the fact. Protesters will need to stay vigilant, and Fight for the Future's Greer emphasizes that everyone has different potential vulnerabilities and tolerance for risk. For people of every category of risk, however, a few thoughtful privacy protections can go a long way towards empowering them to hit the streets.

"Part of the goal of governments extending and implementing mass surveillance programs is to scare people and make people think twice before they speak up," Greer says. "I think that we should be very careful in this moment not to fall into that trap."