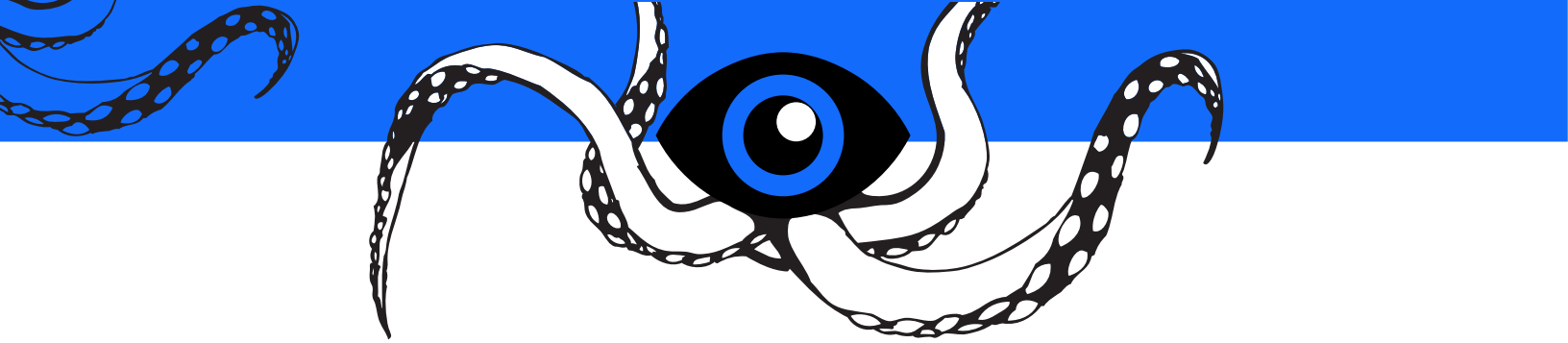

Protest and Digital Self-Defense

The state and private entities are monitoring the digital lives of those who participated in this week's actions to ultimately chill dissent and suppress the rebellion against the systematic racism it upholds.

Practicing basic digital hygiene can offer some protection during political actions such as the demonstrations this week from the state crackdowns that are inevitable in the coming days, particularly against vulnerable communities who are challenging the state's unchecked power to spy and to uphold the murderous status quo against black people. Digital hygiene is an essential element of safety that many ignore because of the normalization of surveillance in day-to-day life.

Privacy is a personal and collective concern and responsibility, not an individual one, and gaps in your digital privacy can have radiating effects on everyone in your network.

Do...

...Leave your digital devices at home. Bringing your phone to an action means that your presence and location can be correlated with it. Furthermore, it can be confiscated and its contents searched.

...Bring a burner phone instead. If you aren't comfortable going phone-free (there are many reasons to bring a phone—being able to get help in an emergency, coordinate with your friends, or document the action), consider purchasing a cheap phone with a prepaid SIM card using cash or a gift card. Do not power on the phone at or near your home. Only install the bare minimum such as an end-to-end encrypted communication app.

...Turn off WiFi and turn off automatic joining of WiFi networks. WiFi networks can track your device's movement from place to place by keeping track of its unique network identifier.

...Keep your device in airplane mode. When your device is in airplane mode, it won't attempt to connect to wireless networks, preventing external tracking of your movements. You can still document the action and can always turn airplane mode off again when you need network access.

...Use end-to-end encrypted, free-software apps to communicate with friends and comrades before, during, and after the protest. It is always best to have in-person communications away from your phones, which can be secretly recording, but if you must have conversations on your phone, use apps that offer end-to-end encryption. Use these same practices when organizing for the action itself.

> Check out: Conversations, ChatSecure, Signal, RIOT, Wire (can all be used for realtime messaging, and Signal, RIOT, and Wire also support voice/video calls)

...Enable full-disk encryption. Full-disk encryption is on by default in iOS, but may need to be enabled manually in the settings on Android. Note that full-disk encryption is only fully effective when the device is powered off.

...Protect your device with a strong PIN or passphrase. Choose a long, random passphrase or PIN to lock your device in case it is confiscated. We recommend generating a PIN of at least 10 digits.

...Set your device to self-destruct after multiple unsuccessful attempts to unlock it. If your phone's operating system offers this feature, take advantage of it to protect against brute-force attacks.

...Enable two-factor authentication wherever possible, preferably via a dedicated app rather than SMS or email. This is especially important for protecting your email and social media accounts, where unauthorized access can be used to breach further online accounts.

Check out: FreeOTP or andOTP

...Power your devices off before a confrontation with police. If you are detained or arrested and are carrying a phone, you may want to power the device off to further restrict access to its contents. However, you need to consider your personal safety and balance the need to protect your digital device with the need to document what's happening, especially surrounding police violence.

...Think before you share. If you are considering posting images or video online, think about your reasons and consider the short- and longterm risks before doing so.

...Keep backups of data you don't want to lose. Consider what information you have on your phone and remove any that could pose a risk to others if compromised.

...Make unique, strong passwords for all your accounts. A password manager can remember and even generate strong, unique passwords for you.

Check out: KeePassXC

Don't...

...Talk to the police. It is never in your interests to make any statement to the police when questioned. Anything you say can potentially be used against you, even if it seems innocuous. Say out loud that you want a lawyer and that you will remain silent.

...Consent to searches of your person or devices. You are not constitutionally or legally required to divulge any passwords, including the passphrase used to lock your phone.

...Protect your device using biometrics. Locking your device using your fingerprint or face is risky, as you can be compelled to unlock the device more easily (even without your cooperation).

...Allow sensitive notifications to appear on your device's lock screen. Limit what information is displayed on your phone's screen when it is locked. It doesn't make sense to use Signal and then reveal on your lock screen sensitive information about your contacts and the topics you are discussing.

...Use SMS or standard phone calls to communicate. These communication methods are inherently insecure and can be intercepted on site using IMSI catchers (a.k.a stingrays), which are now standard equipment for police departments.

...Post photos or videos online before stripping certain metadata. When you take a picture using a phone or digital camera, the resulting file will contain metadata about the device used and GPS coordinates, if available. You can use various free tools to strip this Exif metadata before publishing.

Check out: Exif Tool

...Post pictures of people's faces online without their express consent. Protestors' faces can and will be identified by algorithmic means if these images fall into the hands of surveillance capitalists, such as Google and Facebook, or law enforcement agencies. Make sure the subjects of your photos are willing to take on that risk. If you want to publicly post photos or videos of crowds, make sure to redact faces. Remove as much information about other protestors as possible. Blur faces or, for extra layers of protection, use clone stamp tool or add emojis to hide identifying features.

Check out: Image Scrubber

...Organize via centralized social media platforms. Social media giants such as Facebook/Instagram and Twitter rely on pervasive surveillance of their users as a business model and collude with the state. Consider closing your social media accounts in the long term. If you cannot, remove as much information about yourself as is practical and restrict access as much as possible.

...Organize via other centralized surveillance apparatuses such as Google. Avoid Google and Microsoft's webs of corporate surveillance by, for example, making an email account with a privacy-respecting provider. Encourage your friends and comrades to do the same. What is more, there are other ways to make spreadsheets and share documents for organizing purposes.

Check out: Tutanota, ProtonMail, Cryptpad

...Rely on proprietary apps for comms (or anything else, really). Proprietary software serves its developers first and its users secondarily. These apps will not protect your privacy, as they don't afford you control over your own device. Only rely on free (as in speech) software for sensitive activities.

Avoid: WhatsApp, Telegram, iMessage, Facebook Messenger, Instagram, Google Hangouts, Zoom

Last updated on 2020-06-04 — This advice is subject to change and may be updated as needed.