Infosec 101 for Activists

Drew Bjorn, Mark Sherman, Ph.D., and Blake Skinner

Updated March 27, 2021

Website: https://infosecforactivists.org/ PDF: https://infosecforactivists.org/Infosec_for_Activists.pdf

Introduction

America has a strong tradition of activism, dating back to slave revolts and indigenous uprisings even before the founding of the United States. Today, activism in the US remains critical. Street protests are an essential tool that activists use to raise awareness and push for institutional change. That being said, challenging existing power structures carries an element of risk - exposure can lead to harassment, arrest, or doxxing.

Your personal information is more accessible than it has ever been in the past. In this document, we'll talk about how hostile groups can leverage information against activists, and what you can do to protect yourself and others. This document is focused on digital safety and information security for activists who have special requirements and risks. Others have written about protest safety in a general sense, as well as day-to-day digital safety.

If you are in a hurry, please begin with the tools chart below. You'll find information you can use right away! We have also included tips and concepts to make your personal information safer at actions AND in your day-to-day life.

Why should you care? While challenging existing power structures has always carried an element of risk, the wireless digital landscape provided by today's technology makes it far riskier. Law enforcement commonly works with tech companies to access user data, which the user (you) believed was private. Data breaches expose names and other personal information, which can have ramifications in your everyday life. Our goal is to help you conduct activism safely without bringing unnecessary police surveillance, violence, or threats to your employment to your doorstep. This document is a guide to help you keep control over your own sensitive information.

Tools to Use

Need secure, private communications in a hurry? Here are services you can switch to right now! (We do not receive kickbacks from any of these companies. Or anybody, actually.)

Tools	Use	What it replaces, or what it does	What it costs
BitWarden	Password Manager	Securely saves your passwords so you can use strong and unique passwords.	Free, more features $1/mo
DuckDuckGo	Web Searching	Google Search	Free
DuckDuckGo Maps	Maps, Directions	Google Maps	Free

Tools	Use	What it replaces, or what it does	What it costs
Firefox	Web Browsing	Google Chrome, Safari, Internet Explorer, Edge	Free
Jitsi	Online Meetings	Zoom, Google Meet, WebEx	Free
ProtonMail	Email	Gmail, yahoo, work email	Free, more features $5/mo
ProtonVPN	VPN	Protects your activity from your cable or mobile provider, who may share with police.	Free, more features $5/mo or $10/mo
Signal	Messaging	Text messages, facebook messenger, other insecure instant messaging apps	Free

Tools NOT to Use

In this document, we make recommendations against some popular and commonplace tools. Our recommendations are all based on the same guiding principles. The logic behind them is simple – **avoid tools that collect your information, store it outside of your control, or leave it publicly exposed.** The most challenging is likely Google Maps, which we believe should be avoided while attending an action. Google Maps always tracks its users, and Google keeps this tracking data in detail, forever. All of this data can be given to law enforcement. Police and other agencies can use Google's high-precision data to place a person at an action. Even more dangerous, they can then locate a person down to specific areas within an action, or near criminal acts, within a few feet and down to the minute. Our alternative suggestions, Apple Maps and DuckDuckGo Maps, do not track their users in this way. They also go out of their way to anonymize the data collected by the map providers.

Another popular tool we must recommend against is Telegram, as it has a track record of security issues. While it supports end-to-end encryption for messages between individuals (see Messaging with Encryption below), it does not apply this security to group messages. Group messages may be reported as "spam" or "abuse", and the full contents of messages may be subjected to review by Telegram staff and contractors. That data can then be provided to law enforcement. To make things worse, the full encryption technique is not active for all conversations by default.

WhatsApp, while popular in some activist circles, has similar issues, and we recommend against that service as well. We recommend Signal, which was built from the ground up for personal security.

Similar reasoning applies to all the recommendations we make in this document. If you use it, we have probably researched its security features for this project. If there are tools you are not ready to give up, we encourage you to research their privacy policies and what you can do to protect your data.

Things to Know

Your phone is a data goldmine, full of tracking and identifying information. This includes where you have been, what you have said, and with whom you have communicated with. This section will help you keep that data safe while you are attending a protest, protecting you AND those around you. Find instructions for iPhone and Android below! Get protected and protest-ready right now!

Assume that any messages you send, phone calls you make, or anything else you send or receive can be logged and recorded by the police. If your information is strongly encrypted, they may still have access to it, but they can't decrypt it. Be sure to update your phone to the latest supported operating system (OS) well before the action.

If you have privacy concerns and your phone is no longer receiving software updates, consider not bringing it. If you are attending a protest without a phone, don't go alone. Arrange times and places where you can meet up with your buddies before you go to the protest.

Attending an Action

Before

- Do not mark yourself as "Going" on Facebook.
  - Make note of the details, and save them on a personal device or piece of paper.
- Practice your phone passcode. Enable and practice using Emergency SOS (iOS) and Lockdown mode (Android).
- If you need to search the internet for any information relating to the protest, use DuckDuckGo and private browsing sessions.
- Make sure your device is updated to the latest version of your OS, and all your apps are up to date.
  - Check and update your Android or iOS version to make sure you have the latest security fixes.
- Set up a Signal account. If you don't want to use your personal phone number, you can create a new phone number with Google Voice and register that with Signal.
- Find a friend (or several!) to go with and connect over Signal to discuss plans.

During

- Use a protest buddy.
- Confirm meetup plans with your protest buddies before leaving for the event.
  - Once you meet up, agree on a fallback location in case you get separated.
- Use Apple Maps or DuckDuckGo Maps if you need directions to the location of the protest.
  - If you can, print the directions before leaving for the action. Apple Maps does not have an offline mode, and will not be usable without an internet connection.

After

- Leave and delete Signal groups set up for that protest.
- Don't post your protest photos on social media!

Preparing Your Phone

Your phone is a powerful tool but also a powerful tracking device for law enforcement and other entities. Phones record and share lots of information about your whereabouts and activity with different services. This is usually a good thing, as it helps your apps respond to your needs and situation. But when you attend an action, those features can provide a rich digital breadcrumb trail. We want to prevent those digital breadcrumbs from being dropped, and here is some advice on how to do that.

Attending an action brings an additional threat to privacy. If your phone is lost or confiscated by law enforcement, all the information on it could then be available to police. Below we will share advice to protect your phone against intrusion should it fall into someone else's hands.

This section uses the word "phone" to mean a smartphone running iOS or Android, such as those manufactured by Apple, Google, Samsung, and others. If you are using a simpler phone, your risks are likely fewer.

Digital Breadcrumbs

Whether you have an iPhone or an Android, the threats to your privacy are the same. Your phone has a built-in **GPS** receiver that enables maps and other location-based apps to work. The phone itself will keep that GPS receiver on at all times, recording where you are, and occasionally send updates on your whereabouts to Google, Apple, or other app publishers. So we will want to turn the GPS receiver off, which prevents from the location data from being recorded at all.

Bluetooth and WiFi are common technologies that use short-range radio to communicate with other devices. Unfortunately, their operation requires your phone to broadcast identifiable information about itself. This information can be observed by a "beacon" or scanning device. Stores, government agencies, and police use these devices to identify people who are nearby. This type of surveillance is profoundly dangerous at an action, so we need to disable Bluetooth and WiFi whenever possible.

Your mobile carrier can track your location by when your phone contacts its radio towers. Phones connect to towers periodically while on, even if they are not being actively used. Towers connections are sufficiently accurate to place an individual on the same block as an action. This information can be accessible to law enforcement through a subpoena.

All phones have an option for **"airplane mode,"** which disables *all* radios. This feature was created for travel in an airplane, out of a concern that phones would interfere with the plane's operation. Today it is a reliable way for you to disable all three radios with one button: WiFi, Bluetooth, and mobile carrier. There are some slight caveats, detailed in the iPhone and Android setup instructions, below.

Intrusion Protection

If you attend an action, there is a risk that your phone may be seized by police. They will physically have your phone and may attempt to extract information from it. All phones have **lock screens**, which is the first line of defense. In day-to-day use, we want our lock screen to be prevent a thief or some other stranger from easily opening the phone. With that, fingerprint readers and face scanners make for convenient unlock mechanisms. The situation at an action is starkly different, as law enforcement may have the ability to apply your finger or face to your phone to unlock it, even if you resist or are unconscious. For this reason, **biometric unlock mechanisms should be avoided during an action**. The other unlock mechanisms typically involve drawing a shape or entering a code. A swipe or, shape, or short code can be traced by police (or anyone) from the thin oils your finger leaves on the screen. **Entering a code is the most secure.** The code should be long enough to prevent your fingerprints from giving it away.

Phones also let you select how long they should wait before auto-locking themselves. You should set this time to be as short as possible, so that if you drop your phone or if is stolen, the timer will expire and the phone will lock before anyone else can access it. The **power button should make the phone immediately lock**.

There are ways to access data on a phone without unlocking it. One way to defend against these methods is **full-disk encryption**, where all the information on the phone is stored in encrypted form. This prevents law enforcement from removing the storage chips from your phone, as all of the contents will be unreadable without being unlocked in your specific phone by your specific unlock code.

To use full-disk encryption on an iPhone, simply set a lock screen passcode. If you don't have a passcode, it will not activate the feature.

To see if your Android has encryption available and turned on, you can **go to Settings, choose Security, and find the Encrypt Phone option.** It will say "Encrypted" or prompt you to turn on encryption. Turning on encryption will take a few hours, and your device will need to be plugged into its charger. This is something you only need to do once.

If your Android device was shipped with Android 6 or lower, you may not be able to use this feature.

Phone Backups

Keeping backups of your important data is always a good idea, but the built-in cloud backups of iOS and Android pose a problem for activists. Backups made with iCloud are encrypted in such a way that employees at Apple can access them. This weakness is attributed to pressure from the FBI. Anything in the backup, which may include photos, contacts, unencrypted messages, and more, can be handed over to law enforcement. Keys to unlock the phone's full-disk encryption are also stored in the iCloud backup. This arrangement allows law enforcement to request the backup data from Apple and use the key to unlock the entire phone. It also offers a convenience, where if the user forgets their unlock code, Apple can still recover the device. For activists, the risk posed by your unlock keys being accessible to law enforcement is potentially greater than the benefits of that convenience. **We do not recommend using iCloud backups.**

Android leverages Google Drive for data backup, which does not generally contain unlock keys, but does automatically include app data, call data, contacts, calendar events, videos, and photos. Starting with Android version 9 (codenamed "Pie" and released in 2018), Google has offered end-to-end encrypted backups that even they cannot open without the user's passcode. If your phone uses version 9 or newer, this feature is automatically active as long as you have a lock screen protected with a PIN, pattern, or passcode. **Do not use Android cloud backups prior to version 9.**

Phone Setup Instructions

Below we have specific steps to prepare your iPhone or Android. The goals for both are the same, and are explained above. The buttons to press, however, are quite different between the two. Select the iPhone or Android below to see the instructions.

iPhone Setup

Apple has made personal security a priority in recent years and has provided some iPhone-specific features to make securing your phone easier. These steps can be used to reasonably secure your phone for an action.

- Disable your GPS receiver by turning off Location Services.
  - Even in Airplane mode, iOS will keep the GPS receiver active unless you do this.
  - *Settings* → *Privacy* → *Location Services*, toggle *Location Services* off.
- Turn off Bluetooth, WiFi, and carrier radio by activating Airplane Mode
- Lock screen setup
  - Set your screen to auto-lock as quickly as possible, and require your passcode immediately.
    - *Settings* → *Display & Brightness* → *Auto-Lock*, set to 30 seconds or 1 minute at the most
    - *Settings* → *Touch ID & Passcode*, set "Require Passcode" to "Immediately"
  - Practice with iOS' Emergency SOS mode, and disable the emergency auto-call features.
    - Press and hold the power button and either of the volume buttons until the Emergency SOS lock screen appears. Face ID and Touch ID will be disabled until the passcode is reentered.
    - *Disable Settings* → *Emergency SOS* → *Auto-call*
    - *Disable Settings* → *Emergency SOS* → *Call with Side Button*
  - Disable Touch ID and Face ID
    - *Settings* → *Touch ID & Passcode*, under the section "Use Touch ID For:", toggle all the sliders to off.

Android Setup

Android has flexible settings that can be used to make your phone secure and usable in a number of situations. Below are steps to make your phone generally secure for the day of an action.

- Disable your GPS receiver by turning off Location Services.

  - Pull down the notification panel from the top of the screen. There may be a toggle button for Location Services (they often look like a satellite).
  - If you don't have the button in the pulldown, go to *Settings* → *Location* and turn off "Use location."
- Turn off Bluetooth, WiFi, and carrier radio by activating Airplane Mode.
  - Pull down the notification panel from the top of the screen. There may be a toggle button for Airplane Mode (it often look like an airplane). Ensure Airplane Mode is ON.
  - If you don't have the button in the pulldown, go to *Settings* → *Network & internet* and turn on "Airplane mode."
  - You can turn mobile data back on without leaving airplane mode if you need it. Press the Mobile Data button in the notification panel after you activate Airplane Mode. Those two buttons are often next to each other.
  - Check that Bluetooth is really off. Android may keep it on if Bluetooth devices are connected. The button in the notification panel should be grayed/uncolored to indicate it is off.
- Lock screen setup
  - Go to *Settings* → *Security* → *Screen Lock* and select PIN or Password.
  - You will be asked if you want notifications to be shown on screen while the phone is locked. The safest option is "Don't show any notifications at all." If that does not work for you, choose "Hide sensitive notification content."
  - Click the gear to enter Screen Lock settings:
    * Set "Lock after screen timeout" to Immediately.
    * Turn on "Power button instantly locks".
  - Disable Smart Lock if you have it. It can keep your phone unlocked when you don't expect it, which is dangerous at an action.
- Go to *Settings* → *Display* → *Advanced* → *Screen timeout* and set it to the shortest possible time, usually 15 seconds.

Security Ideas

This section is about keeping your information private in the rest of your life. In this document, "private" means only accessible to you, and not to anyone else without your permission.

Messaging with Encryption

To encrypt your personal communication (like messages with other people), you want *end-to-end* encryption (E2EE). Many apps claim "encryption" but only a few truly guarantee that your information stays encrypted all the way to your recipient's phone. The "end-to-end" means it is only readable by you and your recipient. Without the "end-to-end" property, copies of messages may be sent through and saved on a central server, which the provider company has full access to.

Meeting Online

Virtual meetings over video calls are part of modern life and very common in activist communities. Solutions like Zoom, Google Meet, and Microsoft Teams are popular choices for work and social meetups but do not offer the privacy activism requires. For that reason, we recommend Jitsi. Unlike other platforms, Jitsi does not record or retain the content of your meetings. Jitsi is free and does not even require a user account. You can start a meeting directly from their web page at meet.jit.si. No participants need to have accounts or give any personal information to use the platform. Jitsi takes security and personal anonymity seriously. You can read more on their security page.

Password Safety

The password is the primary mechanism used to secure your online accounts, but it is also a significant point of vulnerability. How can we manage this?

- Turn on two-factor authentication (2FA) everywhere it's offered.
- Use long and strong passwords that are not easily guessed.
- Use a password manager to securely store your passwords, then use a unique password for each service.

Two-Factor Authentication (2FA)

This adds a second check, whenever you log in, that it's really you. The second factor can be an app on your phone, an email, or text message. A one-time-use code is sent to you, which you then enter into the service to prove you control that second factor. Not all channels are equal in their security, but **any 2FA is worlds better than none at all.**

When choosing a 2FA method, a authenticator app such as Google Authenticator provides a good balance between convenience and security. Google Authenticator is free, and available from both the Google Play Store, and Apple's App Store.

If a more secure option is desired, security keys such as the Yubikey can be used. The keys are physical objects which act as your second factor, and can also be used with the Yubico Authenticator can use physical tokens to generate one-time codes.

If the above options are not available for your service, you may be able to use your email or phone (via SMS) to receive one-time codes. These are not as secure as the above options, but, as stated above, any 2FA is worlds better than none at all.

Strong Passwords

Longer passwords are harder to break, regardless of the types of characters they contain. Modern hackers' tools can try every possible character in every order for an 8-character password instantly, but a 10-character password would take hours. XKCD did a fun explanation of this: https://xkcd.com/936/

Your passwords should be easy for you to remember but too long for a hacker to guess. The best technique right now is to use a passphrase of multiple words that are easy for you to remember but so long that it would take centuries for a hacker to crack. You can use a technique called Diceware to come up with a random but memorable passphrase. Doug Muth built a nice online Diceware tool below.

Diceware Password Generator: https://diceware.dmuth.org/

Password Managers

Password managers are apps that work like personal vaults for your passwords. They can save the username, password, and other information for each app and/or site that you use. This vault is heavily encrypted and can only be unlocked by a master password. All you need to remember is the master password, and it will fill in everything else for you! This frees up mental space, which is always nice, but more importantly for security, it allows you to have each site use a completely unique and random password. Most people use variants of the same password or the exact same password across multiple sites and services, and this is a significant security vulnerability. If any of those services are breached (something that is completely out of your control), then your password could be released to the hacker community, often right next to your email. It's shockingly easy for hackers to try using those leaked credentials with other services, including with variations to the password. This is the most common way for people's accounts to be breached. This vulnerability is neutralized if the password used with the hacked service is totally unique.

With a password manager, you can set every service to use a totally unguessable, randomly generated, unique password, like `7Xg*2BMVxCo!uY`. Most password managers include a random generator to make those passwords, and you never have to remember them because they stay securely recorded inside your personal vault within the manager. Our recommendation is BitWarden, an open-source and easy-to-use password manager that uses widely-agreed-upon encryption standards for your passwords.

Security Questions

Services often use personal questions as a backup system, should you need to reset your password. These questions often ask for personal information, like the name of your childhood pet or mother's maiden name. This information, however, is often accessible to others.

When you respond to security questions, try **using code phrases instead of answering them honestly**, so that nobody familiar with your life could guess it and force a password reset without your consent. For instance, for the question "Where did you attend school in the sixth grade?" you could instead respond with your favorite cartoon character from the sixth grade.

Other Tips

These tips don't just protect you, but protect the safety and privacy of others as well!

- Think carefully about who you can safely share your involvement in activism with.
- Don't use email for protest related conversation.
- Google your full name occasionally and see what comes up.
- Do not "check in" to a protest on Facebook or any other service. You don't want to give third parties evidence that you were there. Police use subpoenas to get user information from Facebook and other social media companies all the time.
- Don't take anyone's photo without permission.
- If you take any photos, don't post them on social media. Images have extra information hidden in them that includes the time and place they were taken. If you send photos or videos out at all, only send them to people you trust, over secure means, long after and far away from the protest.
- Have a protest buddy and use Signal to communicate with them.
- When using Signal, enable "Disappearing Messages" for any sensitive conversations.

Closing

We hope that you have found this resource helpful. While at first these materials may seem intimidating, we are confident you can master them with a little time and practice. The world of information security changes frequently and quickly - while we will do our best to keep this page up to date, we encourage you to diversify your information sources.

If you'd like to continue learning, Malwarebyte's Lock and Code podcast has an episode on Why Data Privacy Day matters, and the ACLU tackles ongoing threats to protesters' rights. For ongoing news in the world of privacy and freedom of speech, check out the resources below!

- Techdirt
- Wired: Privacy
- Arstechnica
- EFF Deeplinks

Acknowledgments

Blake, Drew, and Mark would like to thank Clare, Deb, Moe, Sasha, Stacy, and Vincent for their assistance with this project. We also thank our pets, Lacey, Lily, Pico, and Roxy for their support in these challenging times.

Send us feedback (Uses a google form. Do not submit personal or sensitive information.)

Figure 1: