



# SECURING REPRODUCTIVE JUSTICE



**Privacy International & Women on Web's Guide to Digital  
Privacy for Sexual and Reproductive Justice Activists**

<b>DISCLAIMER .....</b>	<b>5</b>
-------------------------	----------

<b>1.CHOOSING MESSAGING SERVICES THAT OFFER END-TO-END ENCRYPTION (E2EE).....</b>	<b>7</b>
---	----------

<b>MANAGING CHAT BACKUP SETTINGS.....</b>	<b>10</b>
---	-----------

<b>MANAGING MULTIPLE SESSIONS.....</b>	<b>12</b>
--	-----------

<b>TWO-FACTOR AUTHENTICATION (2FA).....</b>	<b>15</b>
---	-----------

<b>VISIBILITY SETTINGS.....</b>	<b>18</b>
---------------------------------	-----------

<b>BLOCKING USERS.....</b>	<b>21</b>
----------------------------	-----------

<b>APP PERMISSIONS.....</b>	<b>23</b>
-----------------------------	-----------

<b>MANAGING THIRD-PARTY APPS.....</b>	<b>26</b>
---------------------------------------	-----------

<b>MINIMISING TARGETED ADS.....</b>	<b>28</b>
-------------------------------------	-----------

<b>GOOD GENERAL PRACTICES: DIGITAL HYGIENE.....</b>	<b>31</b>
---	-----------

<b>2.MINIMISING YOUR ONLINE TRAIL AND SECURING YOUR DIGITAL LIFE.....</b>	<b>34</b>
---	-----------

<b>AD/TRACKER BLOCKING.....</b>	<b>35</b>
---------------------------------	-----------

<b>KEEPING YOUR MOBILE PHONE'S LOCATION HISTORY PRIVATE</b>	<b>38</b>
---	-----------

<b>BROWSER PRIVACY SETTINGS.....</b>	<b>41</b>
--------------------------------------	-----------

<b>DISPOSABLE EMAIL ADDRESSES.....</b>	<b>43</b>
--	-----------

<b>ALTERNATIVE FRONTENDS TO MAINSTREAM WEBSITES.....</b>	<b>46</b>
--	-----------

<b>COOKIE MANAGEMENT.....</b>	<b>48</b>
-------------------------------	-----------

<b>PASSWORD MANAGERS.....</b>	<b>50</b>
-------------------------------	-----------



# 5. ADDITIONAL GUIDES

PI has a number of other guides that SRJ activists may find helpful for other aspects of your work including on data protection and for research purposes such as conducting Data Subject Access Requests. Guides include:

PI's Data Protection Guide:

<https://pvcy.org/DataProtect>

The guide is intended to help organisations and individuals improve their understanding of data protection, by providing a framework to analyse the various provisions which are commonly presented in a data protection law.

A guide to Data Subject Access Request (DSAR):

<https://pvcy.org/DSAR>



Data Protection

# 05



DSAR

VPNS.....	53
<b>3.LARGE LANGUAGE MODELS (LLMS).....</b>	<b>56</b>
TWO-FACTOR AUTHENTICATION.....	57
SETTING CHATS TO PRIVATE.....	58
MANAGE ACCESS BY/TO THIRD-PARTY APPS.....	60
STOP YOUR DATA FROM BEING USED TO TRAIN MODELS.....	61
LIMITING ACCESS TO PRIOR INTERACTIONS.....	63
<b>4.PROTECTING YOUR DIGITAL PRIVACY AND PROTESTS.....</b>	<b>65</b>
<b>5.ADDITIONAL GUIDES.....</b>	<b>66</b>



## 4. PROTECTING YOUR DIGITAL PRIVACY AND PROTESTS

SRJ activists might want to organise and/or attend protests to advocate for SRJ issues. However, they need to be aware that increasingly a range of surveillance tools are being deployed by police to monitor and identify activists at protests, like facial recognition technology, IMSI catchers and mobile phone data extraction tools. This means that by attending a protest, the police can potentially identify you, track you and/or monitor you. To help protect yourself from protest surveillance while still exercising your rights, you can consult the following guides:

<https://pvcy.org/LearnSurv>

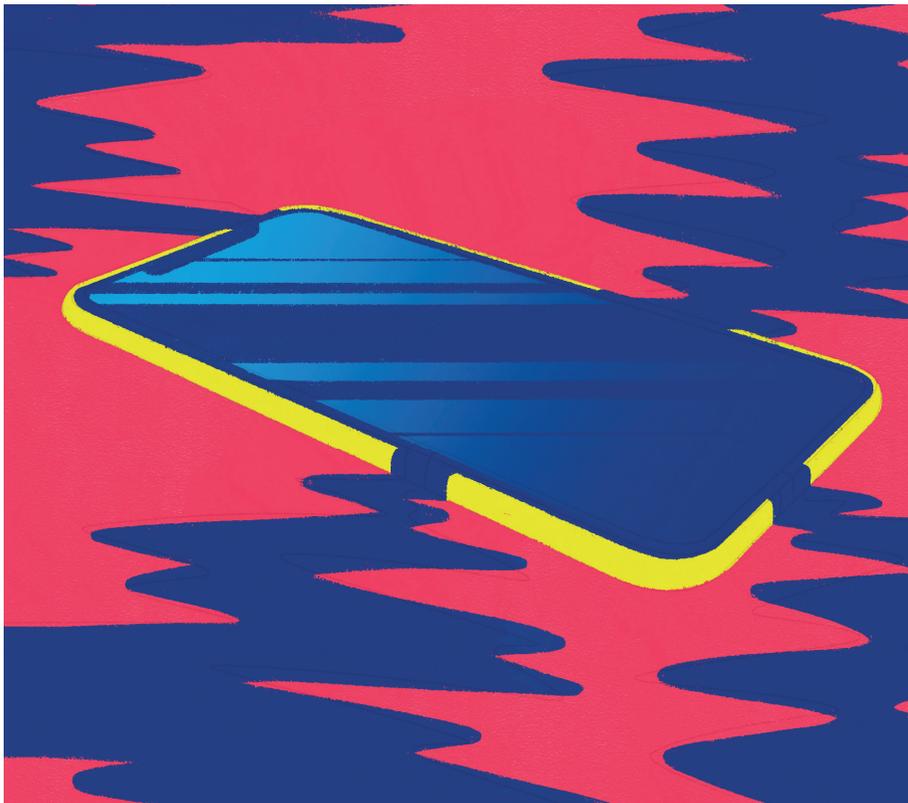
As well as country specific protest guides including UK, Turkey, Pakistan, Colombia and Paraguay.

04



## HOW IT PROTECTS PRIVACY:

- Prevents accidental disclosure of historical data.
- Maintains confidentiality of past activities and communications.



## DISCLAIMER

This guide provides examples of measures to mitigate risks and better protect your privacy. It does not constitute legal advice. As a baseline reference, this guide is not comprehensive, nor does it cover advanced protections.

You can find more and updated guides on Privacy International's website.

Note, while digital and data care is important, please prioritise your physical and mental well-being.

<https://pvcy.org/guide>



# 1. SOCIAL MEDIA AND MESSAGING APPS

Social media and messaging apps are essential tools for SRJ activists, helping with coordination, advocacy, and community building. However, they could potentially expose sensitive personal information and put activists at risk of surveillance. Understanding these risks and implementing good practices allows activists to communicate more securely, better protecting themselves and the people they support.

Remember, while you can take some steps to protect your rights, the platforms are the ones that determine which choices you can make. This guide covers the best practices for the options currently available but stay vigilant as platforms may change their settings (and they often do) with newer versions of apps. For platform specific step-by-step guides that are more frequently updated please visit:

<https://pvcy.org/MessagingApps>

01



## LIMITING ACCESS TO PRIOR INTERACTIONS

### WHY IT MATTERS FOR SRJ ACTIVISTS:

LLMs may retain knowledge from prior sessions that could be recalled later, potentially revealing sensitive strategies or information.

### HOW IT WORKS:

Some platforms store prior interactions that could appear in future sessions, depending on retention policies and settings.

### WHAT YOU SHOULD AIM TO DO:

- Delete or anonymize prior interactions when possible.
- Use private sessions to minimize the storage of sensitive information.

## HOW IT WORKS:

Platforms that use inputs for training may store or aggregate your data. Opting out prevents your contributions from being incorporated into responses provided by future models.

## WHAT YOU SHOULD AIM TO DO:

- Opt out of data collection for training if the platform allows.
- Avoid entering sensitive personal or organizational information if opt-out is not possible.

## HOW IT PROTECTS PRIVACY:

- Prevents activist-related content from being stored or reused in AI models.
- Reduces long-term exposure of sensitive data.

# CHOOSING MESSAGING SERVICES THAT OFFER END-TO-END ENCRYPTION (E2EE)

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Encryption ensures that messages are encrypted between the sender and recipient while in transit. E2EE ensures that only the sender and the recipient have access to the content. For SRJ activists, messages often contain highly sensitive information about individuals seeking care, activist strategies, or internal coordination. Without E2EE, messages could potentially be intercepted and read by:

Governments or law enforcement agencies in restrictive contexts.

Opposition groups.

Malicious hackers and other actors trying to exploit.



## HOW IT WORKS:

Messages are encrypted on the sender's device and decrypted only on the recipient's device. With E2EE not even the company mediating the exchange can read (or listen to) the content, because only the sender and receiver have the capacity to do so.

## WHAT YOU SHOULD AIM FOR:

- Use apps with E2EE enabled by default: Examples include Signal and WhatsApp.
- Enable E2EE manually where needed: On Telegram, use "Secret Chats" for end-to-end encrypted messages.
- Secure devices: Protect your phone or computer with passcodes, biometrics, and disk encryption to ensure messages are not accessible if your device is compromised.
- Minimize metadata exposure: Be mindful of messaging frequency, group composition, and identifying details in communications. Metadata is the information about a message, like the who, when, and where. It's not the actual content of the message itself, but it can still reveal a lot about you.

- Understand the data permissions each app requests before granting access.

## HOW IT PROTECTS PRIVACY:

- Reduces the chance of sensitive data being shared unintentionally.
- Gives you control over who can access information from your LLM interactions.

Stop your data from being used to train models

# STOP YOUR DATA FROM BEING USED TO TRAIN MODELS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

LLM platforms may use the data you input into them via prompts to train models, which can unintentionally include sensitive activist-related content.

# MANAGE ACCESS BY/TO THIRD-PARTY APPS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Third-party apps connected to LLM platforms may access your data or previous inputs. Uncontrolled access can expose sensitive information.

## HOW IT WORKS:

Apps and integrations may request permissions to read or store your LLM data. Regularly reviewing and managing these permissions ensures only trusted apps can access your information.

## WHAT YOU SHOULD AIM TO DO:

- Regularly review connected apps and remove unnecessary or untrusted ones.

## HOW IT PROTECTS PRIVACY:

- Limits anyone from reading or listening to your communications while in transit.
- Supports safer communication with colleagues and individuals you assist.

## IMPORTANT NOTES:

- E2EE is important, but it does not prevent someone from accessing your data if they have access to your unlocked device, to your backups, or to your app's account details.
- Device security is still critical. This means preventing anyone from gaining hands-on access to it which includes not leaving it unattended, using strong measures to protect unlocking, and making sure the device locks automatically when idle.
- It also means protecting access to the data on the device by ensuring that the device is kept secure. The phone's operating system software should be updated and all data stored on the device should be encrypted. Backups should also be encrypted.
- Metadata is not always encrypted and could reveal a lot about the people communicating and allow other forms of tracking.





# MANAGING CHAT BACKUP SETTINGS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Chat backups help with archiving and keeping track of work. However, storing this sensitive information elsewhere can also create additional risks if they are unencrypted or stored insecurely on third-party cloud services. For SRJ activists, backups may contain sensitive information. If unencrypted backups are accessed by governments, opposition groups, or hackers, messages could be exposed.

## HOW IT WORKS:

Most messaging apps offer options to back up chats to the cloud or to a local device. While backups make it easier to recover messages after changing devices or reinstalling apps, not all backups are encrypted. This means that the content of the messages may be accessible to the cloud provider or anyone who gains access to the backup. Local device backups may be safer if the device is encrypted and physically secure, yet still at risk if the device is lost, stolen, or compromised.

## HOW IT WORKS:

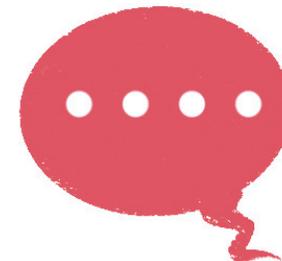
Many LLM platforms allow you to mark chats as private or use restricted sessions that are not visible to other users or third parties.

## WHAT YOU SHOULD AIM TO DO:

- Use platform options to mark chats as private.
- Avoid sharing sensitive information in public or shared sessions.

## HOW IT PROTECTS PRIVACY:

- Limits visibility of sensitive inputs.
- Reduces the risk of exposure to third parties.
- Manage access by/to third-party apps



## WHAT YOU SHOULD AIM TO DO:

- Enable 2FA on all LLM accounts.
- Prefer authentication apps or hardware keys over SMS-based codes.

## HOW IT PROTECTS PRIVACY:

- Prevents unauthorized access even if your password is compromised.
- Keeps sensitive data, communications, and stored interactions secure.

# SETTING CHATS TO PRIVATE

## WHY IT MATTERS FOR SRJ ACTIVISTS:

LLMs can store and process chat data. Keeping chats private prevents others from viewing sensitive conversations or prompts related to activism.

## WHAT YOU SHOULD AIM FOR:

- Evaluate backup necessity: Consider whether you need to back up sensitive chats at all. In some cases, it may be safer not to maintain long-term backups of particularly sensitive conversations.
- Disable cloud backups if the service does not provide encrypted backups.
- Store backups securely: Keep any backups (including those stored locally on devices) protected using techniques including strong passcodes, biometrics, and stored encryption.
- Manage automatic backups: If automatic backups are enabled, regularly review them and ensure they are stored in a secure location or disabled if unnecessary.

## HOW IT PROTECTS PRIVACY:

- Reduces the risk that sensitive communications could be accessed through cloud accounts or compromised backups.
- Ensures that even if your device is lost or accessed, encrypted local backups are much harder to exploit.
- Encourages activists to think critically about which messages need to be preserved, and which should remain only briefly available.

### **IMPORTANT NOTES:**

- Disabling backups can result in permanent loss of messages if devices fail or are replaced, so weigh the risks of data loss versus exposure.
- Regularly review backup settings to ensure they align with your current risk environment and operational security needs.

## **MANAGING MULTIPLE SESSIONS**

### **WHY IT MATTERS FOR SRJ ACTIVISTS:**

Many messaging apps and social media platforms allow users to stay logged in on multiple devices simultaneously. While convenient, this can create a significant privacy risk for activists. If an old or shared device is left logged in, or if someone gains unauthorized access to one of your devices, or can access your passwords and log-in, they could read your messages, access your contacts, or even impersonate you. In a hostile environment, this could put both you and the individuals you assist at risk.

## **TWO-FACTOR AUTHENTICATION**

### **WHY IT MATTERS FOR SRJ ACTIVISTS:**

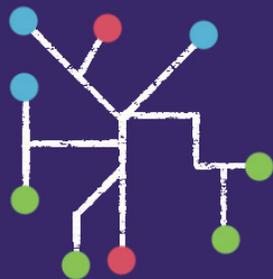
Two-factor authentication (2FA) adds an extra layer of security beyond just a password. This protects accounts from unauthorized access, which is especially important for accounts storing sensitive activist-related information. You can also find more information on 2FA under 'social media and messaging apps' and good general practices'.

### **HOW IT WORKS:**

2FA requires a second verification step, such as a code from an app or a hardware key, in addition to your password.

# 3. LARGE LANGUAGE MODELS (LLMs)

LLMs and AI tools are increasingly used for research, communication, and content generation. However, they can collect and store information from your inputs. For SRJ activists, this could unintentionally expose sensitive information, strategies, or connections. Understanding how to use LLMs safely helps protect both personal and organizational privacy. The following subsections provide practical guidance for safe usage.



# 03

## HOW IT WORKS:

Platforms keep a record of which devices you are using, whether your phone, tablet, computer, or even web browsers. Each “session” is effectively a live login, meaning that anyone with access to that session can interact with your account. Some apps provide notifications or lists of all active sessions, allowing users to monitor and revoke access remotely.

## WHAT YOU SHOULD AIM TO DO:

- Regularly review active sessions by checking your app or account settings to see which devices are currently logged in.
- Log out from or revoke sessions on devices you no longer use or do not recognize.
- Prioritize secure devices by only accessing accounts from devices you trust and control physically.
- Monitor for unusual activity by being alert to notifications about new logins or suspicious sessions. Such notifications may indicate attempted unauthorized access.
- Use session-specific security features such as setting a session expiration time or requiring re-login after a certain time to reduce exposure.

## HOW IT PROTECTS PRIVACY:

- Ensures that only devices you trust can access your messages and accounts.
- Reduces the risk of adversaries gaining access to sensitive communications through forgotten or lost devices.
- Provides greater control over account security and visibility across multiple devices.

## IMPORTANT NOTES:

- Logging out of old sessions does not necessarily remove messages from the devices themselves, so device security (passcodes, encryption) remains critical.
- Some platforms allow notifications for new device logins. Activists should enable these alerts to stay informed of potential breaches.
- Managing multiple sessions is not just a one-time action. In fact, it should be done regularly to maintain operational security.



## IMPORTANT NOTES:

- VPNs do not make you anonymous; they protect traffic but cannot prevent all forms of tracking.
- Be cautious about free VPNs, as some may log activity and/or sell data.
- Legal restrictions on VPN use vary by country; ensure your VPN use is compliant with local laws.
- Sometimes VPN connections may fail or will not work on some networks, so ensure the service running properly.



## WHAT YOU SHOULD AIM TO DO:

- Use a reputable VPN provider with strong privacy policies and no-logs practices.
- Enable the VPN whenever accessing sensitive content or conducting activist work online.
- Be aware that VPNs protect traffic in transit but do not secure activity on devices themselves.
- Regularly update VPN software and review settings for optimal protection.

## HOW IT PROTECTS PRIVACY:

- Encrypts internet traffic, making it difficult for third parties to intercept or read your data.
- Masks your IP address, reducing the risk of location tracking or profiling.
- Enables access to restricted or blocked websites safely.
- Complements other security measures to create a stronger overall privacy posture.



# TWO-FACTOR AUTHENTICATION (2FA)

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Two-Factor Authentication (2FA) adds an extra layer of security to your accounts. Even if someone obtains your password, 2FA makes it much harder for them to gain access. For activists, 2FA is essential because accounts often contain sensitive communications, personal information, and operational data. Without it, a compromised password could lead to serious exposure or harassment.

## HOW IT WORKS:

2FA requires a second form of verification in addition to your password. This could be done via:

- Authentication apps (e.g. password managers) that generate time-based codes.
- Hardware tokens (e.g. YubiKey) that physically verify your presence.
- SMS codes, although these are less secure because they

can be intercepted due to well documented vulnerabilities within the SMS protocol.

When you log in from a new device, the service will prompt you for this second factor to confirm your right of access.

## WHAT YOU SHOULD AIM TO DO:

- Enable 2FA on all accounts that support it, including messaging apps, email, and social media.
- Use authentication apps or hardware tokens instead of SMS whenever possible.
- Secure backup codes in a safe location in case your device is lost or you cannot access the authentication app.
- Regularly review authentication methods and update them if you suspect they may have been compromised.
- Combine with strong passwords: 2FA strengthens security but does not replace the need for unique, random passwords. Generating such passwords is simple when you make use of a password managers (see the guide on password managers!).

# VPNS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

A Virtual Private Network (VPN) redirects your internet traffic through one or more servers, hiding your IP address from the websites you visit and encrypting your data. This can help activists access blocked websites and protect online communications. However, it's important to understand both the benefits and limitations of VPNs.

## HOW IT WORKS:

A VPN routes your internet connection through a server operated by the VPN provider. This process encrypts your traffic and replaces your real IP address with one from the VPN server, making it appear as though your traffic originates from the VPN's location and effectively hides your home IP address.



## HOW IT PROTECTS PRIVACY:

- Prevents account compromise due to weak or reused passwords.
- Reduces the risk of unauthorized access to personal or activist-related accounts.
- Protects sensitive communications, documents, and online interactions.
- Provides a secure and organized way to manage multiple accounts safely.

### IMPORTANT NOTES:

- Choose a password manager with strong encryption and a good reputation.
- Keep the master password secure and never share it.
- Even with a password manager, remain cautious of phishing attempts and device security.
- Ensure the password manager's vault is backed up securely somewhere in case your device is lost or stolen and you need to set up again.
- You will want to know or otherwise safely-store the password for your vault (and the password to the back-up device/service).

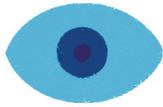
## HOW IT PROTECTS PRIVACY:

- Adds an additional barrier against unauthorized access, even if a password is compromised.
- Reduces the risk of account takeover and the potential consequences for both activists and the people they support.

### IMPORTANT NOTES:

- SMS-based 2FA is vulnerable to interception and SIM-swapping attacks, so it should be used only as a last resort.
- 2FA does not protect the content of your messages on a compromised device, so device security remains crucial.
- Activists should treat 2FA as part of a broader digital hygiene strategy, alongside encrypted messaging, device security, and session management.
- Ensure you have setup your 2FA with care, to ensure that you can access the second factor, e.g. if your device is lost or stolen, because you can lock yourself out of your account. Password managers and good backups are crucial.





# VISIBILITY SETTINGS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Controlling who can see your social media profile, posts, and personal information can be crucial for activists. Publicly visible content can be used by adversaries, opposition groups, or even governments to track, identify, or target activists and the individuals they support. Visibility settings help minimize exposure and reduce the risk of harassment, doxxing, or surveillance. (Note: doxxing refers to the act of publicly revealing someone's private or identifying information [such as their real name, address, or contact details] without their consent, often with the intent to harass or intimidate them.)

## HOW IT WORKS:

Most social media platforms allow users to adjust:

- Profile visibility: Who can view your profile or personal details.
- Post visibility: Who can see individual posts, stories, or updates.
- Friends/followers lists: Who can view the people you are connected with.

## HOW IT WORKS:

A password manager is a secure digital vault that stores your passwords and other private credentials. It encrypts this information and allows you to generate strong, unique passwords for each account. Many password managers also include features like two-factor authentication support, automatic form-filling, secure notes, and breach alerts.

## WHAT YOU SHOULD AIM TO DO:

- Use a reputable password manager to randomly generate and store strong, unique passwords for every account.
- Do not use the same password for multiple platforms/sites.
- Avoid storing passwords in browsers or unencrypted documents.
- Use the password manager's security features, such as breach monitoring, to stay informed of potential risks.



- Prevents third parties from building detailed profiles based on your activity.
- Reduces the risk of linking online activity to your identity or networks.
- Helps maintain control over the data stored on your devices.

### IMPORTANT NOTES:

Some websites may require certain cookies to function correctly; in that case you might need to selectively allow necessary cookies, and continue browsing with that in mind.

## PASSWORD MANAGERS

### WHY IT MATTERS FOR SRJ ACTIVISTS:

Passwords are the primary protection for your accounts and sensitive information. Activists often manage multiple accounts across email, messaging, social media, and organizational platforms. Weak, non-random or reused passwords increase the risk of unauthorized access, which can compromise both personal and activist-related data. Password managers help create strong, random, unique passwords and store them securely.

Location tagging: Whether your posts include location data.

By adjusting these settings, you control the audience for your content and limit the amount of personal information available to unknown parties.

### WHAT YOU SHOULD AIM TO DO:

- **Be mindful of personal details:** Avoid including information in profiles or posts that could reveal your identity (for example avoid using your full legal name in your username or profile), workplace, or locations of activism. You could also choose to have an account to conduct your activism that is separate from your personal account.
- **Consider setting profiles to private:** Only approved followers or friends should be able to view your information.
- **Limit post visibility:** Use settings to share posts only with trusted groups or individuals.
- **Disable location tagging:** Prevent platforms from sharing your physical location in posts or stories. There is more information on disabling location settings under the guide “Minimising your Online Trail and Securing Your Digital Life”.
- **Review connections:** Periodically audit followers, friends, and group memberships to ensure you only share information with trusted individuals.

## HOW IT PROTECTS PRIVACY:

- Reduces the chance of being identified, tracked, or targeted online.
- Minimizes exposure of your networks and contacts to potential adversaries.
- Helps protect sensitive personal and organizational information from unwanted access.

## IMPORTANT NOTES:

- Even with private settings, screenshots, and data leaks can still expose content, so always assume that any post could be seen outside your intended audience.
- Visibility settings should be reviewed regularly, as platform updates can change defaults or add new features that affect privacy.



## HOW IT WORKS:

Cookies store data such as login information, site preferences, and browsing behaviour. Third-party cookies allow companies to track you across multiple websites, building detailed profiles. By managing cookies, you can limit this tracking, delete stored data, and prevent future collection.

## WHAT YOU SHOULD AIM TO DO:

- Enable automatic cookie deletion or regularly clear cookies from your browser.
- Use browser settings or extensions to block third-party cookies.
- Employ auto consent tools to help manage cookie consent forms more efficiently.
- Review and adjust cookie preferences for websites you use frequently.

## HOW IT PROTECTS PRIVACY:

- Limits tracking across websites and reduces the amount of data collected about your browsing habits.

## IMPORTANT NOTES:

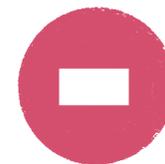
- Some features of the main platform may not be available on alternative frontends.
- The security and privacy of frontends depend on the provider; choose reputable options and avoid logging in by sharing your password.
- Combining alternative frontends with other privacy strategies strengthens overall protection.

# COOKIE MANAGEMENT

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Cookies are small files that websites store on your browser to remember information about your visits. While some cookies are necessary for basic website functions, others track your activity across sites for analytics or advertising purposes. For activists, cookies can reveal browsing habits, interests, and connections, which could be used to profile or monitor your activities. Managing cookies helps reduce exposure and protect privacy.

# BLOCKING USERS



## WHY IT MATTERS FOR SRJ ACTIVISTS:

Blocking users can be an important tool for maintaining a safe online environment. Activists may face harassment, threats, or targeted probing from opposition groups, trolls, or unknown individuals. Allowing harmful accounts to remain connected increases the risk of exposure, intimidation, or manipulation, which can compromise both personal safety and the safety of the people activists support.

## HOW IT WORKS:

When you block a user on a social media or messaging platform:

- They cannot see your profile, posts, or stories.
- They cannot send you messages or interact with your content.
- Some platforms prevent them from tagging or mentioning you.

Blocking contributes to cutting off an unwanted connection. It will not necessarily prevent them from setting up a new account and connecting again.

## WHAT YOU SHOULD AIM TO DO:

- Block suspicious or harassing accounts: Don't wait for repeated incidents, early action reduces risk.
- Document instances of harassment and report them when appropriate: Platforms often provide options to report threatening or abusive behaviour.
- Review followers and contacts periodically: Remove or block users who are unknown, suspicious, or no longer relevant to your activist work.
- Use group-level controls: On platforms that allow it, restrict who can join groups or comment on posts.
- Educate peers: Encourage colleagues to also use blocking and reporting tools to maintain collective safety.

## HOW IT PROTECTS PRIVACY:

- Stops direct harassment and limits unwanted interactions.
- Limits the exposure of personal information to potential adversaries.
- Helps maintain a controlled and safer online network for activism.

## WHAT YOU SHOULD AIM TO DO:

- Use privacy-respecting frontends when accessing mainstream platforms for reading and sharing content or public discussions (e.g. <https://yewtu.be/> for <https://youtube.com> or <https://nitter.net> for <https://x.com>)
- Verify the credibility and security of any frontend before use to avoid introducing new risks.

## HOW IT PROTECTS PRIVACY:

- Reduces data collection by the main platform and third-party trackers.
- Limits the amount of personal information exposed during browsing.
- Helps prevent profiling and monitoring based on online activity.
- Provides a safer way to access content without directly interacting with the primary site.

# ALTERNATIVE FRONTENDS TO MAINSTREAM WEBSITES

## WHY IT MATTERS FOR ACTIVISTS:

Platform websites such as YouTube or X often collect extensive data on users, including browsing habits, location, and engagement patterns. For activists, using these platforms directly can expose sensitive activity or networks to profiling and surveillance. Alternative frontends provide a way to access and share content without directly interacting with the primary site or forcing your audience to do so, reducing the amount of personal data shared.

## HOW IT WORKS:

Alternative frontends are third-party services or interfaces that allow you to view content from popular platforms without logging in, executing tracking scripts, or exposing your identity. These services typically strip out ads, trackers, and other features that collect data, giving you a more privacy-conscious browsing experience.

## IMPORTANT NOTES:

- Blocking is not a guarantee of complete privacy; blocked users may still attempt to create new accounts or access content through mutual contacts.
- Well-resourced adversaries can use social-media intelligence services and firms to monitor large numbers of users, particularly when their accounts are not restricted.

# APP PERMISSIONS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Apps often request access to sensitive device features such as your location, contacts, camera, microphone, or storage. Sometimes this seems convenient, or we don't pause to reflect on what this means before granting permission. However, for activists, granting unnecessary permissions can expose personal information, reveal networks of contacts, or enable tracking. Limiting app permissions reduces the risk that sensitive data about your work or the people you assist is collected or misused.



## HOW IT WORKS:

Each app on your device can request permission to access certain functions such as your contacts, camera or location. Granting these permissions allows the app to potentially use these features, even when you are not actively interacting with it. Permissions vary by device, platform, and app. Some apps may leak data from your device to their servers or share the data with third parties.

## WHAT YOU SHOULD AIM TO DO:

- **Review permissions regularly:** Check which permissions each app has and revoke any that are unnecessary, even if they seem convenient.
- **Grant the minimum required permissions:** Only provide access to features essential for the app's functionality.
- **Be cautious with sensitive features:** Limit access to location, contacts, camera, microphone, and storage unless absolutely necessary.
- **Use device permission managers:** Many devices have built-in tools to monitor app activity and restrict permissions dynamically.
- **Educate team members:** Ensure everyone in your organization or network follows the same principles to reduce collective exposure.

## HOW IT PROTECTS PRIVACY:

- Separates sensitive or temporary activity from your main email account.
- Reduces the risk of profiling or linking online actions to your identity.
- Limits exposure to spam, phishing, and surveillance.
- Provides greater control over who can contact you and how your email data is used.

## IMPORTANT NOTES:

Disposable emails are not suitable for all communications. Some services may reject them if a verified account is required.

Do not share personal details when using disposable addresses.

Consider using trusted services with a clear privacy policy; some free disposable email providers may still log usage or share data.



## HOW IT WORKS:

Disposable email services generate temporary addresses that forward messages to your real inbox or exist only for a limited period. These addresses can be used for registrations, newsletters, or communications where you do not want to reveal your permanent email. Once discarded, the disposable address prevents further emails from reaching you and limits tracking or profiling tied to that address.

## WHAT YOU SHOULD AIM TO DO:

- Use disposable email addresses for sign-ups, online forms, or communications where permanent identification is unnecessary.
- Avoid linking disposable emails to personal accounts or identifiable information.
- Rotate addresses regularly to reduce exposure over time.
- Consider combining disposable emails with other privacy measures, such as encrypted messaging and tracker blockers.
- Store any essential information from disposable email accounts securely if needed before discarding them.

## HOW IT PROTECTS PRIVACY:

Minimizes the personal and operational data that apps can collect.

Reduces the risk of tracking by third parties, including advertisers or adversarial actors.

Helps prevent inadvertent exposure of contacts, locations, or sensitive activist work.

## IMPORTANT NOTES:

Some app functionality may be limited if permissions are revoked, so balance security with operational needs.

Permissions should be reviewed periodically, especially after app updates, as new features may request additional access.



# MANAGING THIRD-PARTY APPS

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Third-party apps often request access to your social media or messaging accounts to provide extra features or analytics. For activists, granting access to third-party apps can create serious privacy risks. These apps may collect sensitive data, monitor your communications, or share information with advertisers or unknown parties. In hostile environments, this could lead to targeting, harassment, or exposure of the people you support.

## HOW IT WORKS:

When you authorize access to/by a third-party app, you typically grant it permissions to read certain account information, post on your behalf, or access contacts. These permissions may be permanent until manually revoked, and the apps can potentially store or share the data outside your control. Examples of third-party apps include (but are not limited to) social media management platforms or artificial intelligence (AI) assistant apps.

## IMPORTANT NOTES:

- Private or incognito modes do not hide your activity from your internet service provider, networks, or the websites you visit.
- Some websites may require cookies or scripts to function properly; consider selective exceptions rather than fully disabling.
- Combining browser privacy settings with ad/tracker blocking, VPNs, and careful online behaviour provides stronger protection.

# DISPOSABLE EMAIL ADDRESSES

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Email is a key channel for communication, but it can reveal your identity, associations, and activity patterns. For activists, using a permanent email for sensitive communications can increase exposure to surveillance, phishing, or profiling. Disposable email addresses provide a layer of separation, allowing you to interact online without linking activity to your main accounts.

## WHAT YOU SHOULD AIM TO DO:

- Enable browsers' tracking prevention and content blocking features.
- Block third-party cookies and disable unnecessary scripts.
- Limit or disable browser telemetry and data-sharing features.
- Use private or incognito modes when appropriate, though they do not prevent all tracking.
- Regularly clear browsing history, cache, and cookies.
- Consider using privacy-focused browsers or extensions to strengthen protections. You can find some examples by following links to step-by-step guides on PI's website.

## HOW IT PROTECTS PRIVACY:

- Reduces the ability of websites and third parties to track your activity across the web.
- Limits the collection of device and behavioural data.
- Prevents automatic profiling based on browsing habits.
- Provides a safer, less exposed online environment for research, communication, and activism.

## WHAT YOU SHOULD AIM TO DO:

- Review connected apps regularly: Check which third-party apps have access to your accounts.
- Revoke access for unneeded or untrusted apps: Remove any app that is not essential or does not come from a trusted provider.
- Limit app permissions: Only grant the minimum access required for functionality.
- Avoid sharing credentials: A third-party app with access to your password becomes a significant security risk.
- Educate your network: Ensure team members or collaborators follow the same practices to reduce collective exposure.

## HOW IT PROTECTS PRIVACY:

- Maintains control over who can access your accounts and data.
- Reduces the risk that sensitive communications or contacts are exposed.
- Minimizes the chance that adversaries or advertisers collect information from your accounts.

## IMPORTANT NOTES:

- Even after revoking access, some apps may retain previously collected data. Be aware of app privacy policies.
- Regularly auditing third-party apps should be part of ongoing digital hygiene practices.
- Managing third-party access complements other privacy measures such as strong passwords, session management, and end-to-end encryption.

## MINIMISING TARGETED ADS

### WHY IT MATTERS FOR SRJ ACTIVISTS:

Targeted advertising relies on collecting personal data, online behaviour, and interests to serve tailored content - a practice commonly known as surveillance-based advertising. For activists, this data could reveal sensitive interests, networks, or activities, potentially allowing adversaries to monitor or profile you and the individuals you support. Minimising targeted ads reduces the amount of data platforms collect about you and makes it harder for others to track your online behaviour.

## BROWSER PRIVACY SETTINGS

### WHY IT MATTERS FOR SRJ ACTIVISTS:

Browsers are the gateway to your online activity, and default settings often allow extensive tracking and data collection. For activists, this can reveal sensitive information about the websites you visit or the content you access. Adjusting browser privacy settings helps reduce exposure to surveillance, profiling, and data collection.

### HOW IT WORKS:

Browsers can track your activity through cookies, scripts, telemetry, and other features designed to enhance user experience or serve personalized content. These mechanisms collect data about your browsing habits, device, and location. By configuring privacy settings, you can block or limit trackers, prevent telemetry collection, and control how websites interact with your device.

## HOW IT PROTECTS PRIVACY:

- Prevents detailed records of your movements from being stored or shared.
- Reduces the risk that your location could expose networks, meeting points, or sensitive activities.
- Limits profiling by third parties, advertisers, or adversaries.
- Helps protect the privacy and safety of the people you work with.

## IMPORTANT NOTES:

- Some emergency or cellular services may still transmit approximate location even with GPS disabled.
- Deleting location history from cloud accounts may not remove all backups - always verify deletion.
- Exposure by one person in your network can impact others; encourage colleagues to manage their own settings as well.

## HOW IT WORKS:

Platforms use data like search history, interactions, likes, and demographic data to show ads tailored to your profile. By adjusting your privacy and advertising settings, you can limit the use of your data for personalized advertising. This does not block ads entirely, but it prevents platforms from creating detailed profiles based on your activity.

## WHAT YOU SHOULD AIM TO DO:

- Turn off ad personalization on platforms such as Facebook, Instagram, Google.
- Limit data sharing within apps: Avoid connecting accounts across platforms unnecessarily.
- Adjust interests and ad preferences: Remove or edit interests that could reveal sensitive topics.
- Review platform settings regularly: Updates may change defaults or add new tracking features.
- Use privacy-focused account features: For example, “Off-Facebook Activity” or ad activity review tools to limit how your data is used for targeting.

## HOW IT PROTECTS PRIVACY:

- Reduces the chance that platforms build detailed profiles linking you to activism or sensitive topics.
- Minimizes exposure of your networks, contacts, and behaviour to advertisers or potential adversaries.
- Limits the digital footprint that could be exploited for targeting or harassment.

## IMPORTANT NOTES:

- Turning off ad personalization does not eliminate all tracking or profiling, but it significantly reduces detailed targeting.
- Regularly revisiting settings is important, as platform policies and features change over time.
- This strategy complements other privacy practices such as encrypted messaging, session management, and strong visibility controls.



## WHAT YOU SHOULD AIM TO DO:

- Turn off location history and background location tracking in your device settings.
- Only grant location permissions to apps when absolutely necessary - which is rarely if at all - and limit use to when the apps are actively in use.
- Avoid posting location information in social media, or embedding them in photos or communications related to sensitive activities.
- Review and delete stored location history from devices and cloud backups regularly.
- Use offline or privacy-respecting navigation apps where possible.
- Consider a separate device without linked accounts for sensitive meetings or travel.



# KEEPING YOUR MOBILE PHONE'S LOCATION HISTORY PRIVATE

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Mobile phones constantly generate location data through GPS, Wi-Fi, Bluetooth, and cellular networks. For activists, this data can reveal movement patterns, meeting locations, and connections, potentially exposing sensitive activities or networks to surveillance or adversaries. Managing location data is essential for maintaining privacy and operational security.

## HOW IT WORKS:

Phones and apps track your location whenever sensors are active, often in the background. This data can be stored locally on your device, shared with other people, uploaded to cloud accounts, or shared with third-party apps and services. Even without actively sharing your location, automatic backups, app integrations, and social media check-ins can retain or transmit this information.



# GOOD GENERAL PRACTICES: DIGITAL HYGIENE

## WHY IT MATTERS FOR SRJ ACTIVISTS:

Even with strong privacy settings, encrypted messaging, and controlled visibility, daily online habits can significantly impact your security. For activists, small lapses like oversharing personal information, reusing passwords, neglecting device security, or falling for phishing attempts can expose sensitive data about your work, your contacts, or the individuals you assist. Good general practices help establish consistent digital hygiene and reduce the likelihood of surveillance, harassment, or data leaks.

## HOW IT WORKS:

Digital hygiene involves routine actions that protect your accounts, devices, and communications. By consistently applying these habits, you reduce the risk that adversaries can exploit your data or compromise your online presence.

## WHAT YOU SHOULD AIM TO DO:

- Use strong, unique passwords for each account.
- Enable 2FA on all accounts to add an extra layer of security.
- Keep software up to date: regularly check for security updates available for your apps and devices.
- From time to time re-evaluate whether a platform is still secure for continued use. Apps often make changes to their terms of service which could affect how they use your data.
- Be cautious with links and downloads: Avoid clicking on suspicious links or opening unknown files.
- Stay educated on phishing methods: Learn to recognize fake login pages, deceptive emails, and impersonation attempts, and verify unexpected messages before responding.
- Think critically before posting and before creating your account: Avoid sharing identifiable information, locations, or sensitive content publicly.
- Reevaluate your situation: Periodically review older posts and consider archiving or deleting content you no longer feel comfortable with.
- Regularly review account activity: Check login sessions, connected apps, and privacy settings. Stay aware of platform updates or policy changes.
- Educate peers and networks: Sharing good digital hygiene practices strengthens collective security.

- Be aware of limitations: Blocking trackers reduces profiling but cannot eliminate all forms of data collection or surveillance.

## HOW IT PROTECTS PRIVACY:

- Reduces the collection of data that could identify or target activists and the individuals they assist.
- Minimizes exposure to targeted ads and profiling across platforms.
- Provides more control over your digital footprint and online behaviour.

## IMPORTANT NOTES:

- Blocking trackers does not guarantee anonymity on its own. Combine with other privacy measures such as privacy-preserving networking or virtual private networks (VPNs). Note, there is a standalone guide on VPNs.
- Some websites may not function fully when trackers are blocked so you might need to consider whitelisting trusted sites if necessary.
- Ad and tracker blocking should be part of an ongoing digital hygiene routine, not a one-time setup.

This blocking can occur at several levels:

- **Browser level:** Extensions or built-in browser features block trackers, prevent cross-site tracking, and stop personalized advertising while browsing.
- **Device level:** System-wide privacy settings or privacy-focused apps can block trackers across all apps on iOS, Android, macOS, Windows, and Linux.
- **Network level:** Tools like Pi-hole block tracking domains for all devices connected to your network, providing an additional layer of protection and reducing exposure to surveillance across multiple devices.

## WHAT YOU SHOULD AIM TO DO:

- **Enable tracking protection in browsers:** Use privacy-focused settings or extensions to block third-party trackers.
- **Use system-level privacy settings:** Adjust device settings to limit tracking and app access to identifiers and personal data.
- **Consider network-level blocking:** If feasible, tools like Pi-hole can help block trackers for all devices in a household or organization.
- **Regularly review and update blocking tools:** Tracker technologies evolve constantly, so keep extensions, apps, and systems up to date.

## HOW IT PROTECTS PRIVACY:

- Reduces the risk of account compromise, data leaks, or exposure of sensitive information.
- Limits opportunities for adversaries to track, profile, or target activists or the people they support.
- Supports a proactive and sustainable security culture within activist networks.

## IMPORTANT NOTES:

- Habits should be maintained consistently. Digital hygiene is an ongoing process, not a one-time action.
- Be vigilant and careful. Small oversights, such as password reuse or ignoring suspicious activity, can create vulnerabilities.



## 2. MINIMISING YOUR ONLINE TRAIL AND SECURING YOUR DIGITAL LIFE

Every little digital action such as a message sent, a website visited, or a file stored in the cloud, leaves traces that can reveal patterns about who you are, what you do, where you are, and who you work with. For activists, these traces can become vulnerabilities if they're collected, analysed, or misused by governments, corporations, or opposition groups. Minimising your online trail isn't about going offline, it's about understanding how information moves, what gets stored, and how to reduce exposure without compromising your work.

Below are practical areas to focus on to strengthen your privacy and security in daily digital life.

# 02

## AD/TRACKER BLOCKING

### WHY IT MATTERS FOR SRJ ACTIVISTS:

Online platforms often gather information about how you use their services to serve you with ads - a practice also known as surveillance-based advertising. For activists, this can lead to profiling that exposes your networks, interests, or activities to third parties. Ad and tracker blocking helps you limit the amount of personal data collected about you and reduces the ways in which you can be monitored or targeted online.

### HOW IT WORKS:

Trackers are small pieces of code, often invisible, that follow your online activity across different sites and apps. They record what pages you visit, what you click on, and sometimes even your location or device details. This data is then used to build detailed behavioural profiles, often shared or sold to advertisers and data brokers. Ad and tracker blockers work by detecting and blocking these elements before they can load, stopping the data collection at its source.