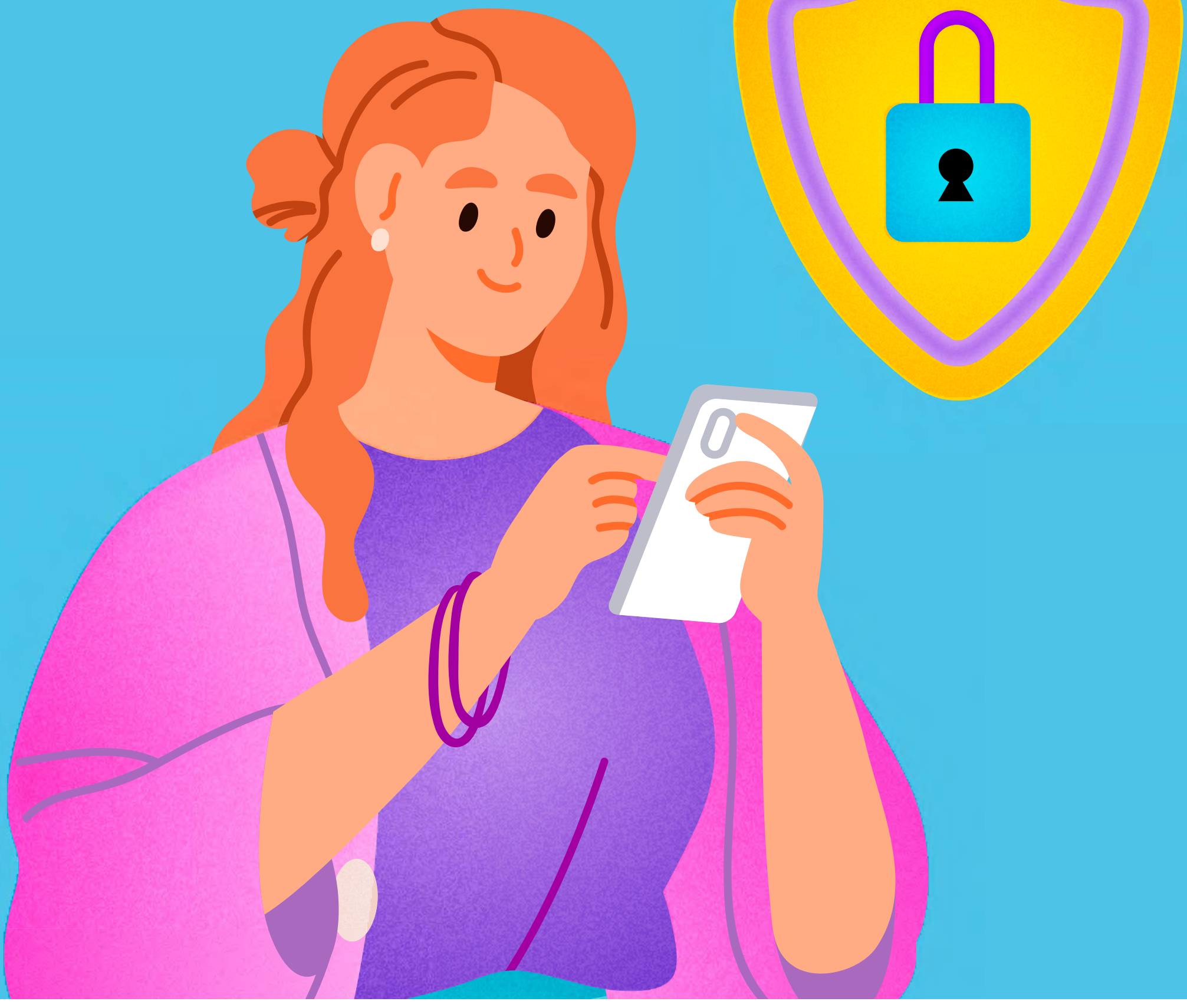
Digital Security for Abortion

How to Protect Your Privacy



CYBER COLLECTIVE

safe2choose.org

how to use abortion pill

Looking for abortion information but worried about your online privacy?

You're not alone!

Accessing abortion services can be challenging, particularly in restrictive areas, but staying informed and safeguarding your digital security is essential. We have prepared practical tips to help protect your privacy throughout the process.

Let's get started!

1. Looking for abortion services or information online

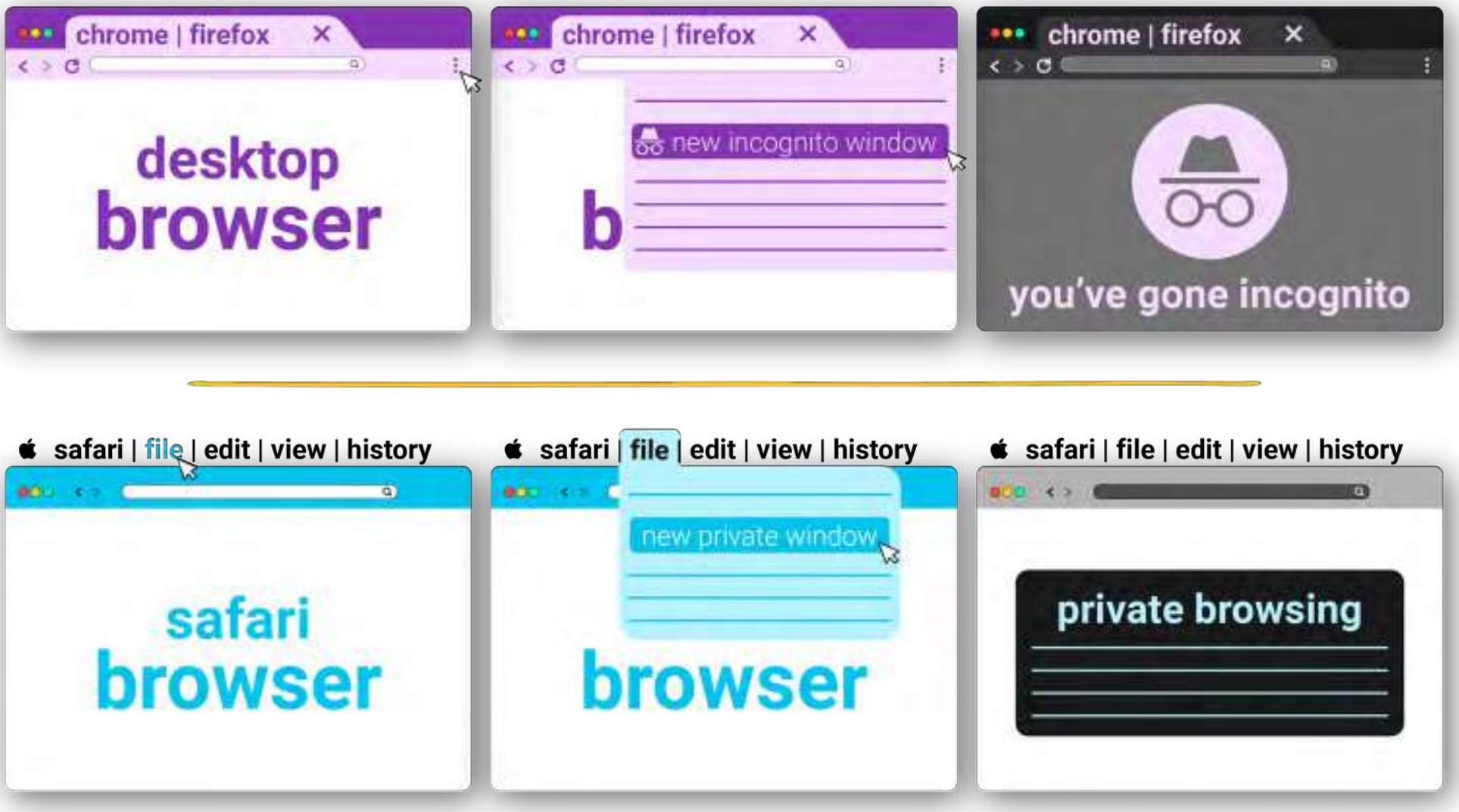
It’s important to know that internet browsers are not private. Big Tech companies record your online moves and use them to target you with ads. These records can be shared with authorities if requested (although usually they need a warrant).

What can you do to protect yourself?

- Using a VPN will make your internet navigation safer and more private.
  - A VPN (virtual private network) encrypts your data and masks your IP address, protecting your browsing activity, identity, and location. If you’re looking for greater privacy and autonomy, a VPN is the right choice.

Note: Encryption is a technology that protects data by scrambling it into a secret code that is only accessible with a unique digital key.

- Use a privacy-focused browser like Firefox Focus, Tor Browser, or DuckDuckGo. If you can't download one, you can use incognito mode to prevent your browser from saving your browsing history, cookies, and site data, keeping your activities private on shared devices. While it doesn't prevent tracking entirely, it reduces data storage. When you're done, simply close the incognito/private window to end the session.
  - On most desktop browsers, you will find the incognito mode option in the top right corner by clicking on the three dots or dashes and selecting "New incognito window." On Safari, you will have to click on "File" in the menu bar, and select "New incognito window."

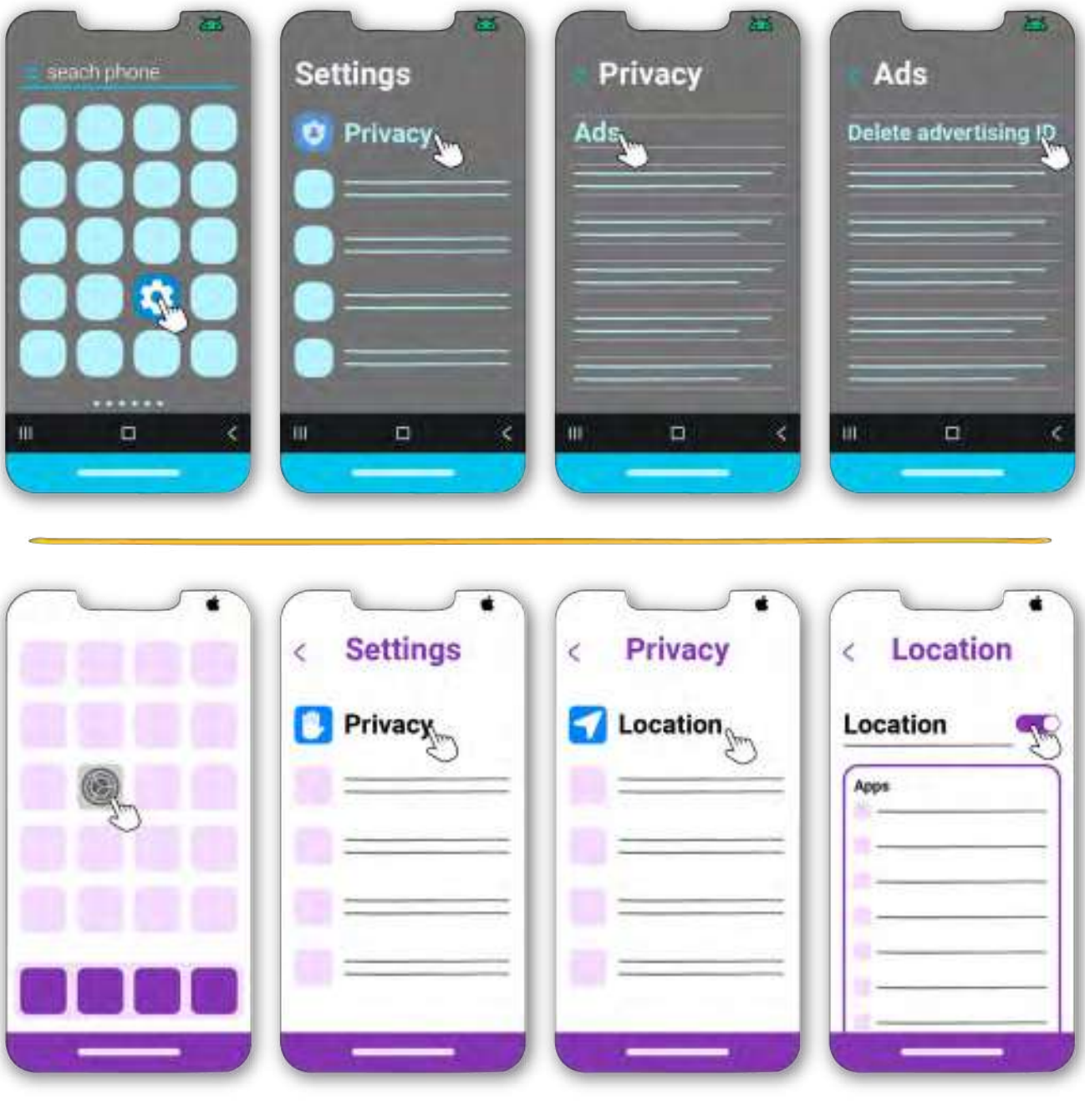


- It also works on mobile browsers: tap the three dots or dashes and select “New incognito tab.” On Safari, tap the tab icon and select “Private” to open a new private browsing tab.

- Disable your mobile ad ID and opt out of ads. Companies like Google and Meta (Meta is the owner of Facebook, Instagram, and WhatsApp) track your online activity for targeted advertising; blocking them ensures you have more privacy on the platforms.

  - To delete your advertising ID on Android devices, go to Settings > Privacy > Ads. Tap “Delete advertising ID” and confirm. This will prevent apps from accessing it in the future. This option may not be available on older versions of Android. If you can’t find it, go to the privacy settings to reset your ad ID and request that apps not track you.

  - On Apple devices, when you install a new app, it may request permission to track you. To manage this, go to Settings > Privacy > Location Services and you can disable tracking for individual apps that you’ve previously allowed.



- Big Tech companies have made it harder to access safe abortion information. Always check the information and reputation of the abortion services you find online as there are many scammers and fake clinics (for example, crisis pregnancy centers).
    - If the instructions seem absurd, including long periods of fasting and intense physical exercise, be suspicious. During an abortion with pills, it is important to eat and stay hydrated.
    - An abortion is a very safe procedure. If the information only highlights the risks or is full of images of fetuses, it may be a fake clinic.

2. What to do when contacting: organizations, counselors, abortion providers, or clinics through (online) messaging services

Family members, your partner, or even friends might read your SMS messages on your phone or through your account if they have access to your phone bill. When using messaging services, even if you delete your messages, messages will be stored and could be shared with authorities, if requested (again – they usually need a warrant).

What can you do to protect yourself?

- Use a strong PIN or password on your devices. If possible, create an alphanumeric password, mixing upper- and lowercase letters.

- Avoid using X, Tiktok, Facebook, and Instagram for sensitive conversations.

- If possible, use Signal, which is a safe, independent nonprofit messaging and calling app that does not store images to your device. Do not forget to turn on disappearing messages on Settings > Privacy > Disappearing messages. If you are an IOS user, also switch off “Show Calls in Recents” on Settings.

- When you are texting or calling regular numbers, use a prepaid phone or make use of a VOIP, a type of internet telephone service, instead of your personal one (try an app like Hushed).

- If this is not possible, calls and messages through apps like Signal, WhatsApp, or Telegram are encrypted and more secure than ordinary phone calls and SMSes.

- Do not forget to set up disappearing messages for all these conversations, including with close friends and family.

    - Go to Settings > Privacy and tap “Default duration.” > Select 24 hours or 7 days.

- Do not save the provider's contacts on your phone. If you must save the contact, use a random name that does not attract attention. On WhatsApp, you can also lock the conversation.
  - To do so, on Android, tap and hold the conversation you want to lock. Tap the three dots at the top right, and then tap "Lock chat." You can also create a secret code to access this conversation.
  - On IOS, hold down on the conversations and you will see different options, including "Lock chat."

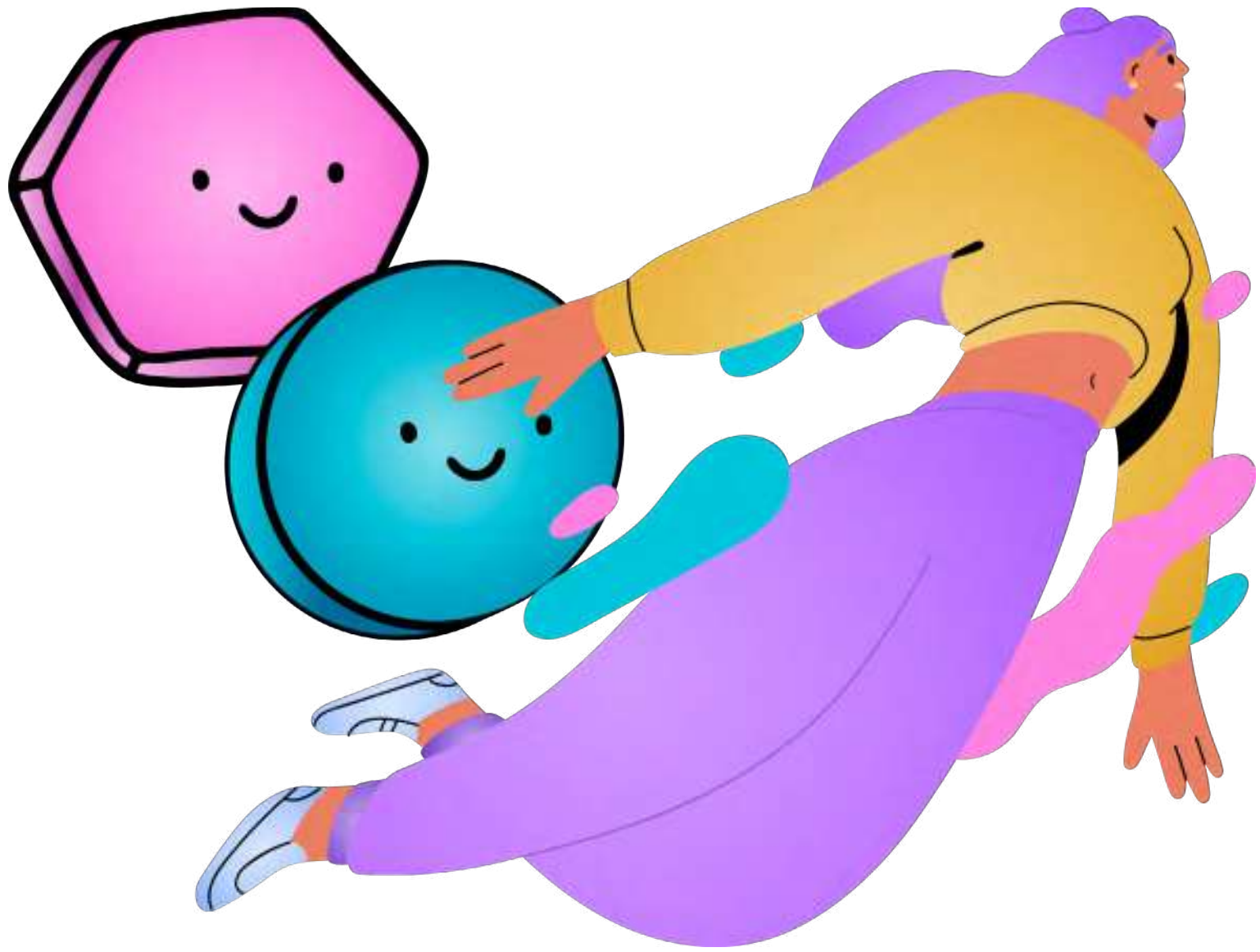
- When emailing, use a secondary email address that's not linked to any of your existing accounts and delete it afterwards. You can create an account on Proton Mail. It encrypts all your emails so the people who hold your account (Proton Mail) cannot access what is inside, and emails from outside providers (like Gmail, Hotmail) also get encrypted immediately.

- Avoid taking and sharing screenshots of these conversations and saving compromising images on your device. You can also use the view once feature on WhatsApp when sending images and voice messages, ensuring they disappear from the chat after the recipient has opened them once.

    - Select "view once" every time you send a voice message, photo, or video by clicking on the icon with the number one in the text bar. (1)

Attention: when paying for abortion services or medical care, try to use cash to avoid cards and bank transfers being tracked. If a prepaid card is available in your country, it's a good option.

Note: Are you using your browser to contact abortion providers? Protect your digital security and privacy with the security measures from step 1 – use a privacy-focused browser, browse in an incognito window, or opt out of ads.



3.

Accessing abortion services

(by visiting a provider, getting abortion pills, etc.)

Family members, your partner, or even friends might read your SMS messages When accessing abortion services, you will likely have your mobile phone with you. However, your phone transmits signals which means your location can be tracked. Mobile operators can provide this information to authorities, if it's requested.

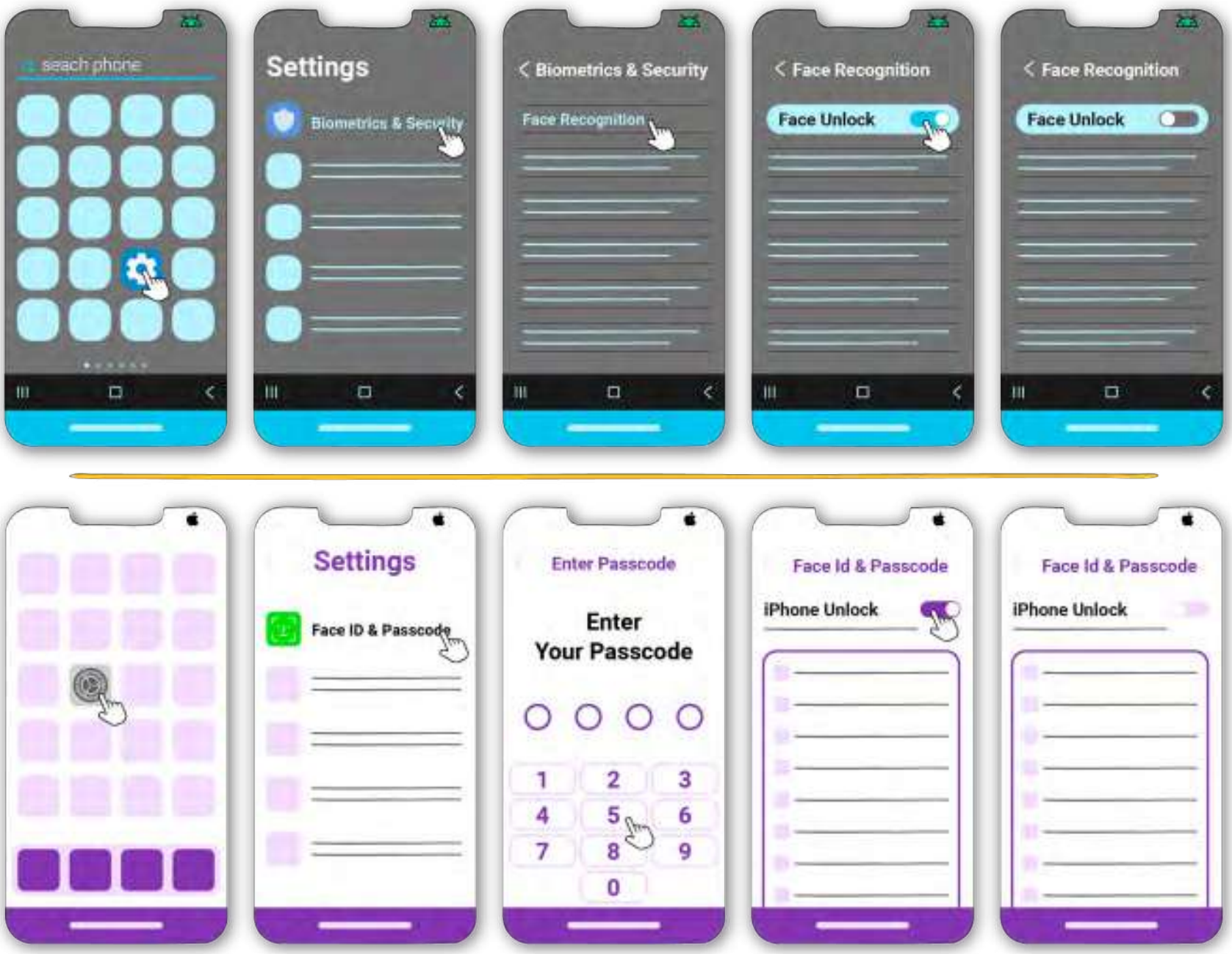
What can you do to protect yourself?

- Your phone can be tracked by its network signal, Wi-Fi, GPS, Bluetooth, and possibly other methods. The best option is to turn off your phone completely and have someone you trust with you.

- If it's not possible, at least consider turning off your location sharing:
  - On Android, go to Settings, tap “Location,” click on “Access my location” and turn it off.
  - On IOS, go to Settings, then tap on “Privacy & Security” and switch off “Location Services.”

  - If you are traveling by car and are not sure if it has technology that tracks your location, consider using public transportation or parking away from the place you have to go to.

- Consider turning off face ID or fingerprint, especially if there is a risk of having your device seized.
  - On Android, go to Settings, then to “Biometrics & password,” choose “Fingerprint” and/or “Face recognition,” tap your phone password and switch it off.
  - On iOS, go to Settings, then tap “Face ID & Passcode”, go to “Use Face ID” and disable “iPhone unlock” or “iPad unlock.”



- If possible, avoid using navigation apps to reach the address, such as Google Maps or Waze. If that's not possible, make sure they aren't saving your route in their history.

- If needed, you can clean your data on Google Maps by opening the Google Maps app and tapping your profile picture or initial. Click on “Your data” in Maps, then “Web & App Activity: See and delete activity.” When you see the entries you want to delete, tap “Remove.”

- If you are looking for a safer alternative altogether, try OsmAnd, an offline map application that does not save your data.

Share this information
with anyone who might need it.

Let's make access to abortion safer for everyone!

References:

1. "Keep Your Abortion Private & Secure." *Digital Defense Fund*, 2021, www.digitaldefensefund.org/ddf-guides/abortion-privacy/. Accessed October 2024.

2. "Practical Guide to Strategies and Tactics for Feminist Digital Security." CFEMEA, 2017, www.cfemea.org.br/index.php/pt/radar-feminista-lista/livros-guias-e-estudos2/4670-guia-pratica-de-estrategias-e-taticas-para-a-seguranca-digital-feminista. Accessed October 2024.

3. "Abortion Access Activist, Worker, or Patient." *SSD*, www.ssd.eff.org/playlist/reproductive-healthcare-service-provider-seeker-or-advocate. Accessed October 2024.

4. "Digital Privacy Tips for Abortion Seekers." *Asian Americans Advancing Justice*, 2022 www.advancingjustice-aajc.org/digital-privacy-tips-abortion-seekers. Accessed October 2024.

5. "Digital privacy for your private parts." *Vagina Privacy Network*, 2019 www.vaginaprivacynetwork.org. Accessed October 2024.

6. "A certification for online abortion counselors." *safe2choose*, www.safe2choose.org/abortion-counseling/online-abortion-training-course. Accessed October 2024.

7. Gómez. Noelia. "Digital conservatism: search engines' strategy to hide information about abortion." *La Política Online*, 2024, www.lapoliticaonline.com/politica/los-buscadores-incentivan-el-conservadurismo-digital-y-suprimen-informacion-sobre-el-aborto/. Accessed October 2024.

8. "Internet Street Smarts Course". Cyber Collective, www.cybercollective.org/internet-street-smarts. Accessed November 2024.

DIGITAL SECURITY FOR ABORTION

This manual was produced in collaboration by **HowToUseAbortionPill, Cyber Collective ad safe2choose.org**.

HowToUseAbortionPill is an online community run by dedicated individuals who believe that everybody, regardless of where they live, should have access to a safe abortion option. **www.howtouseabortionpill.org/**

Cyber Collective makes it easier for people to feel safer, secure and confident in their digital experiences NOW—so that we can have a better future. **www.cybercollective.org/**

safe2choose is a digital eHealth platform dedicated to empowering individuals with accurate, confidential, and compassionate abortion care and information. **https://safe2choose.org/**

Illustrations and graphic design by Ana Ibarra. **www.behance.net/anafriedbanana**

Endorsed by:

CENTER FOR INTIMACY JUSTICE

© 2024 HowToUseAbortionPill, Cyber Collective & safe2choose. All rights reserved.

CYBER COLLECTIVE safe2choose.org how to use abortion pill