PROTECT YOUR PRIVACY WHEN SEEKING ABORTION CARE

The right to abortion under California law is well established and safe abortion care is available here in the state. Below are some steps to better protect your privacy when accessing abortion care, especially if you are coming from out of state to seek an abortion in California. Included at the end of this alert are several additional resources that may provide further technical guidance.

BE CAREFUL WHO YOU TALK TO ABOUT YOUR SEARCH FOR ABORTION CARE

- If you are not a resident of a state that protects your right to abortion, limit the discussion of your search for abortion care. Only disclose your search to medical professionals and other trusted persons.

KEEP YOUR INTERNET SEARCHES AND ONLINE ACTIVITY PRIVATE

- Use a device that you trust and on which you can control the search methods. Do not perform your search on a device owned or operated by another person or entity, such as at work, a library, or internet cafe.
- Consider using a virtual private network (VPN). VPNs encrypt (hide) your internet traffic on unsecured networks to help protect your online identity. There are VPN options available online for free or low cost, for use on your computer, mobile device, and home WiFi network.
- Use a web browser on your phone and computer that protects your privacy, including by not storing your browsing history. If you cannot avoid using a web browser that stores your browsing history, go to the web browser settings and use the clear or delete history feature to delete all cookies, cache, and browsing history. Then, go to the browser settings and select private or incognito browsing. Also, while in settings, select the option for blocking cookies.
- Consider using a more private search engine, like DuckDuckGo or Qwant, and a more private internet browser like Firefox Focus or Brave. Do not use a search engine that has an option where you can create an account associated with your personal information (such as your email address), and definitely do not log into such an account when searching.

LIMIT YOUR MOBILE DEVICES' TRACKING FEATURES

- If possible, do not bring a web, cellular, or GPS connected device with you when travelling to or inside an abortion clinic. If you must bring such a device with you, follow the steps below to limit being tracked by your device. Steps to avoid tracking include:

  1. Turn off location sharing on your phone and mobile device. Limit how apps can access location data by setting location permissions in your phone or device settings.

     - For Android users, go to S*ettings > Personal > Location Access. Then, turn off "access to my location."*
     - For Apple users, go to Settings > Privacy > *Location Services. Switch the toggle to off.*

- *Note*: because ride-share apps like Uber and Lyft link a person to a location, you may want to be prepared to make other transportation arrangements.

2. Disable the mobile advertising identifier (mobile ad ID) on your phone and mobile device. A mobile ad ID is a unique identifier associated with your phone that is used to track your online activity.
   - For Android users, go to Settings > Privacy > Ads. Tap "Delete advertising ID," then tap it again on the next page.
   - For Apple users, go to Settings > Privacy > Apple Advertising. Then set "Personalized Ads" toggle to the "off" position. Also, go to Settings > Privacy > Tracking. Then set "Allow apps to Request to Track" toggle to the "off" position.
3. Because social media apps may automatically leave you logged in, even when you are not actively using the app, log out of and do not use social media on the days you are traveling to or visiting a clinic.
4. Turn Bluetooth off on your phone and mobile device when not in use, and use it in "hidden" mode rather than "discoverable" mode.
5. Be careful about connecting to public WiFi and adjust your device settings so it does not automatically connect. Consider disabling WiFi to avoid inadvertently putting your sensitive information stored on your device and in online accounts at risk.
6. Disconnect activity trackers, such as smartwatches, from location services, or do not wear them on the days you are traveling to or visiting a clinic.
7. Avoid taking photos with your phone camera on the days you are traveling to or visiting a clinic. Even with location tracking turned off on photos, the contents of photos can still reveal your location.

Keep Emails Private

- Do not use an email associated with your job or school.
- Use an email service that protects your privacy by using end-to-end encryption. With end-to-end encryption, only the sender and recipient can read the communication. While most popular free email services offer some encryption, end-to-end encryption is not the default and a user must take steps to enable it.
- Consider creating a new email address that is not linked to your regular email account for emails related to abortion services. Enable the disappearing messages feature, or use a disposable email (a temporary email address that self-destructs after a single use or a defined period of time).

Keep Your Text, Voice, and Social Media Messages Private

- For messaging, only use 3rd party apps that use end-to-end encryption, instead of your phone's default messaging service.
- Review the messaging app's privacy policy to ensure it does not track, collect, or sell your information.

- Follow the instructions in the messaging app or on social media messaging to enable the disappearing messages feature.
- Delete messages once you no longer need them.

Keep Payment Transactions Private

- If you are not a resident of a state that protects your right to abortion, pay for abortion-related care in cash if possible. If paying in cash is not possible, use cash to purchase a prepaid card, instead of using a credit or debit card. Do not provide contact information when making the prepaid card purchase.

ADDITIONAL RESOURCES

- Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet, U.S. Department of Health & Human Services
- Seeking an abortion? Here's how to avoid leaving a digital trail, Washington Post,
- In A Post-Roe America, Googling "Abortion" Could Put You At Risk. Here's How To Protect Yourself, BuzzFeed
- Protecting Your Privacy in the Post-Roe US, CNET
- Freaked Out? 3 Steps to Protect Your Phone, The New York Times
- Tech Tip: How to securely send email and texts, USA Today
- Your apps are watching everywhere you go unless you change this setting, USA Today
- A Simple Way to Make It Harder for Mobile Ads to Track You, WIRED

FREQUENTLY ASKED QUESTIONS
PROTECT YOUR PRIVACY WHEN SEEKING ABORTION CARE

This seems like a lot of steps. Why is this so complicated?

A lot of information can be collected from your online and offline activities in today's interconnected world. This can include your location, web browsing, searches, and purchases.

Many apps access your location, such as to provide a list of nearby restaurants, directions to a friend's home, or a local weather forecast. What you may not realize is that some apps track your location all the time, even when you are not using them, by accessing your geographic information from GPS, WiFi, and cell tower networks.

Companies may also make certain inferences about you based on the products you search for or purchase, such as inferring when you are pregnant based on specific product purchases.
All this data that is collected about you may then be sold to entities known as "data brokers." Data brokers often combine and resell personal information bought from many sources.

While companies may claim that they only sell de-identified information (i.e., data about you, but with contact and demographic information removed), studies show that de-identified information can often be re-identified.

Although in some instances you may be okay sharing your personal information, it may not be desirable if you are seeking abortion care. If you want to protect your privacy, follow the steps above.

Should I turn off my smartwatch or my phone while I am at the clinic?

Yes, or even better do not bring your phone, smartwatch, or any other web-connected device to the clinic. If you do bring any web-connected devices, turn off location services before traveling to the clinic.

What about period tracking and pregnancy apps?

Recent news reports have suggested that several period (menstrual cycle) tracking and pregnancy apps are selling or sharing personal information with advertisers and data brokers. If you use these apps, carefully review the app's privacy policies to determine whether they sell or share any personal information.

If you want to stop using one of these apps, under California law known as the California Consumer Privacy Act you have the right to delete your personal information and delete the app from your mobile device. If you wish to continue using the app, you have the right to opt-out of sale of your personal information.

What if my privacy was breached?

You can contact the Attorney General's Public Inquiry Unit to file a complaint. https://oag.ca.gov/contact/consumer-complaint-against-business-or-company.

***

This consumer alert was issued by the Healthcare Rights and Access (HRA) Section of the California Department of Justice. HRA works proactively to increase and protect the affordability, accessibility, and quality of healthcare in California. HRA's attorneys monitor and contribute to various areas of the Attorney General's healthcare work, including consumer rights; anticompetitive consolidation in the healthcare market; anticompetitive drug pricing; nonprofit healthcare transactions; privacy issues; civil rights, such as reproductive rights and LGBTQ healthcare-related rights; and public health work on tobacco, e-cigarettes, and other products.