CONSUMER ALERT

Protecting data privacy when seeking reproductive health care

AUGUST 2023

REPRODUCTIVE RIGHTS UNIT
OFFICE OF THE SOLICITOR GENERAL
ARIZONA ATTORNEY GENERAL KRIS MAYES

Consumer Alert:

Tips for Protecting Your Data Privacy When Seeking Reproductive Health Care

In today's digital world, a lot of information can be collected from people's online and offline activities, including location, web browsing history, searches and purchases. For example, many apps access location in order to provide a list of nearby stores, map directions or to report the weather forecast. In fact, whether you realize it or not, some apps are tracking your location even when the app is not in use. Tracking in the background occurs by accessing geographic information from WiFi, GPS and cell tower networks. Companies may also make certain inferences about users based on the products searched and bought online.

Although sharing this sort of personal information in some instances may not bother some people, many may want greater control over their digital footprint and how their data can be collected by third parties. In the reproductive health care space in particular, data privacy has become a concern for those seeking care. Even though abortion is currently legal in Arizona up to 15 weeks, and past that under some circumstances, many people may wonder how to protect their privacy when seeking reproductive health care.

If you or a loved one is searching for or currently accessing legal reproductive care, including abortion care, consider taking steps to protect the privacy of your data. A digital footprint cannot be completely erased, but the following tips can help ensure that information and data remains private.

ATTORNEY GENERAL
STATE OF ARIZONA

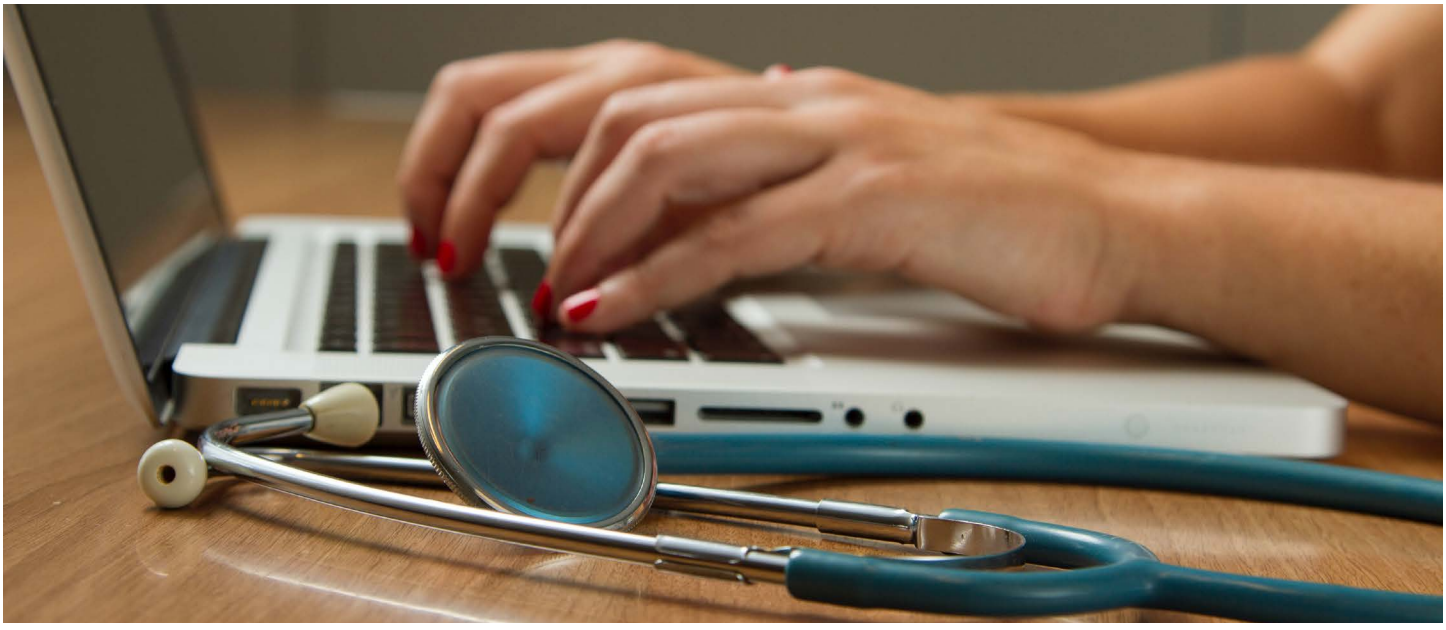
Be mindful of who you talk to about your search for abortion care.

When looking for abortion care, only disclose the search to licensed medical professionals and trusted people in your life.

HIPAA

Information is not protected simply because it's healthcare-related. The Health Insurance Portability and Accountability Act (HIPAA) only protects medical and health information when it is transmitted or maintained by certain entities like health plans, most healthcare providers or the business associates that provide services for those entities.

In other words, HIPAA is not a blanket protection for any and all health information and discussions. Importantly, HIPAA does not protect internet search history, geographic location information, or information voluntarily shared online. HIPAA usually does not protect data downloaded or entered into apps, unless the app is specifically provided by a covered entity or its business associate. When in doubt, speak with a medical provider about how information will be treated in any specific situation.



Keep internet searches and online activity private.

TRUSTED DEVICE

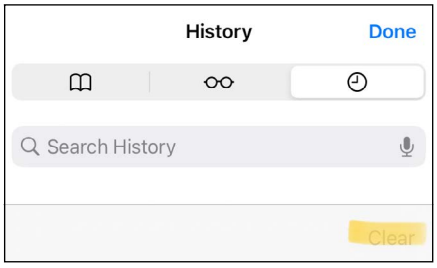
When searching the internet for information and resources, use a trusted device to control the search methods. Do not conduct a search on a device owned or operated by another person or entity, such as at work, a library or a public computer.

VPN

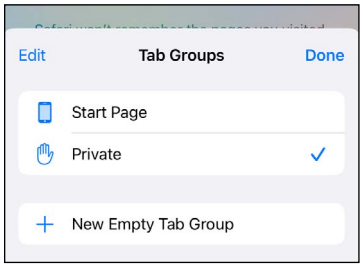
Consider using a virtual private network (VPN) for internet searches. VPNs encrypt internet traffic on unsecured networks to help protect online identities. There are free or low-cost VPN options available for use on a computer, mobile device and home WiFi network.

BROWSING HISTORY

When searching the internet on a phone or computer, use a browser that protects privacy by not storing browsing history. If a web browser that stores browsing history cannot be avoided, follow these steps:



Go to the web browser settings and use the "Clear History" or "Delete History" feature to delete all cookies, cache, and browsing history.



While in browser settings, select the option for "private" or "incognito browsing."

In browser settings, select the option for blocking cookies.

SEARCH ENGINES AND BROWSERS

Consider using a more private internet browser and search engine. Do not use a search engine that has an option to create an account associated with personal information, such as an email address. And definitely do not log into such an account when searching.

Examples of private internet browsers: Firefox Focus or Brave
Examples of private search engines: DuckDuckGo or Qwant

Limit tracking features on mobile devices.

If possible, do not bring a web, cellular or GPS connected device, including a smart watch, when traveling to an abortion clinic. If you must bring such a device, follow the steps below to limit how devices track your movements.

Steps to avoid tracking:

TURN OFF LOCATION SHARING ON A PHONE AND MOBILE DEVICE

Limit how apps can access location data by setting location permissions in the phone or device settings.

Android users: Go to Settings > Personal > Location Access. Turn off "access my location."

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, consider arranging other transportation as available.

DISABLE THE MOBILE ADVERTISING IDENTIFIER

Disable the mobile ad ID on phones and mobile devices. A mobile ad ID is a unique identifier associated with your phone that is used to track online activity.

Android users: Go to Settings > Privacy > Ads. Tap "Delete advertising ID," then tap it again on the next page.

Apple users: Go to Settings > Privacy > Apple Advertising. Set "Personalized Ads" toggle to the "off" position.

Go to Settings > Privacy > Tracking. Set "Allow apps to Request to Track" toggle to the "off" position.

LOG OUT

Patients should log out of, and not use, social media on the day they travel to a clinic. Social media apps may automatically leave users logged in, even when the app is not in active use, and can gather location data in the background.

TURN BLUETOOTH OFF

Turn Bluetooth off on phones and mobile devices when not in use, and use it in "hidden" mode rather than "discoverable" mode.

PUBLIC WIFI

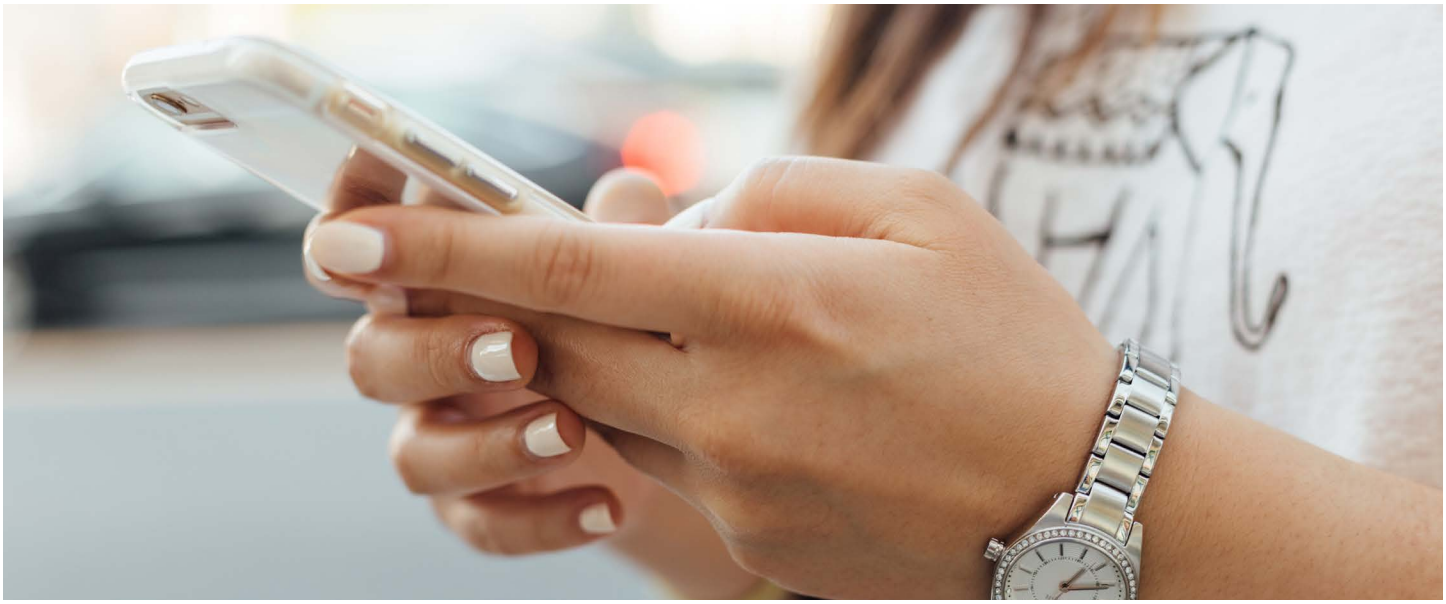
Adjust device settings to not automatically connect to public WiFi. Consider disabling WiFi completely to avoid unintentionally putting sensitive information stored on the device and online accounts at risk.

ACTIVITY TRACKERS

Those seeking reproductive health care should disconnect activity trackers such as smart watches from location services, or do not wear them on the days they travel to or visit a clinic.

PHOTOS

Avoid taking photos with a phone camera on the days of an appointment. Even with location tracking turned off, the contents of photos can reveal a patient's location.



Keep emails private.

PICK UP THE PHONE

As much as possible, consider using phone calls, instead of email, to gather information and communicate with others about accessing care.

ENCRYPTION

Do not use an email associated with a job or school. Use an email service with end-to-end encryption that protects privacy by allowing only the sender and recipient to read the communication. While most free email services offer some encryption, end-to-end encryption is not the default and a user must take steps to enable it.

SEPARATE EMAIL ADDRESS

Consider creating a new email address that is not linked to a regular email account for emails related to abortion services. Enable the disappearing messages feature with a permanent email address. Or use a temporary email address that self-destructs after a single use or a defined period of time.

Keep text, voice and social media messages private.

THIRD-PARTY APPS

For messaging, only use third-party apps that use end-to-end encryption, instead of a phone's default messaging service.

PRIVACY POLICY

Review messaging app privacy policies to ensure it does not track, collect or sell information.

DISAPPEARING MESSAGES

Follow the instructions in the messaging app or on social media messaging to enable the disappearing messages feature. Delete messages once they are no longer needed.

Keep payment transactions private.

CASH

Pay for abortion-related care in cash. 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.

AVOID CASH APPS

Avoid using payment apps like Venmo or Cash App. If a cash app must be used, make sure the account is set to private so transactions are not public.

Use caution with period-tracking apps.

Recently, news reports have suggested that some period-tracking and pregnancy apps are selling or sharing personal information with advertisers and data brokers. Carefully review the privacy policies of these apps.

If you wish to stop using one of these apps, review the privacy policies to determine whether you can request they delete personal information and whether you can opt out of the app selling your personal information to third parties.

Do research.

Data privacy — both in the reproductive health care space and more broadly — continues to be an evolving issue, and the law does not always keep pace. It's important to do research and stay plugged in to developments in this area to protect yourself.

Among the many resources available online, the U.S. Department of Health and Human Services has compiled a list of sources[1] on data privacy.

- Federal Trade Commission resources on protecting privacy[2] while using apps.
- Guidance from the National Security Agency on limiting location data exposure[3].
- Reviews from Consumer Reports on data practices[4] of various electronic products.

What if my privacy was breached?

FILE A COMPLAINT

If you believe a company has gathered your information in violation of its privacy policies, or has misused or sold your information without authorization, you can file a complaint[5] with the Arizona Attorney General.

If you need a complaint form sent to you, contact the Attorney General's Office.

PHOENIX	TUCSON	OUTSIDE METRO
(602) 542-5763	(520) 628-6648	(800) 352-8431

NOTE: Bilingual staff are available to assist and answer any questions.

Bottom line.

These tips do not guarantee digital anonymity. Nor are they intended to frighten you or chill you from engaging in lawful activities, including seeking reproductive health care. What matters is that you understand how data might be collected and shared, and educate yourself on how you can manage your digital footprint to the best of your ability, based on your comfort level.

LINKS

1 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
2 https://consumer.ftc.gov/articles/how-protect-your-privacy-apps
3 https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF
4 https://www.consumerreports.org/issue/data-privacy
5 https://www.azag.gov/consumer

KRIS MAYES

REPRODUCTIVE RIGHTS UNIT
OFFICE OF THE SOLICITOR GENERAL
ARIZONA ATTORNEY GENERAL KRIS MAYES

AUGUST 2023