A Student's Guide to Reproductive Data Privacy

The Ethical Tech Initiative @ The George Washington University Law School

Introduction to Student Reproductive Data Privacy

The Ethical Tech Initiative @ The George Washington University Law School

After the Supreme Court ruled in 2022 that bans on abortion do not violate the US Constitution, many states criminalized abortion. Depending on the state, this means that anyone who has or helps facilitate an abortion (including doctors and nurses, Lyft drivers, and patients themselves) are potentially criminally liable. Whether you are or could become pregnant, or have friends, relatives, or patients who are or could become pregnant, the criminalization of abortion is very concerning. The scope of criminal liability is wide: people could be prosecuted for a range of activities connected with reproductive health—including something as simple as an online search for information about a pregnancy test or reproductive health care services. There are also significant concerns about privacy and the sharing of otherwise protected intimate data.

While no privacy measures are foolproof, this pamphlet sets forth some simple things you can do to reduce the

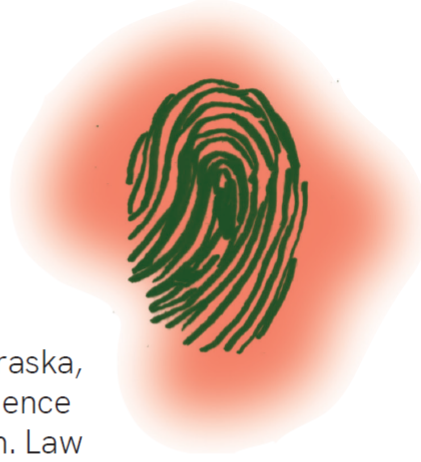
risk of unwanted disclosure of your personal reproductive and other private data.

For most students like you, smartphones and laptops are a necessary part of your daily routine. You trust your browser to remember passwords to important accounts, credit card information, and other personal information. While, for most of us, there's no getting rid of technology completely, it's important to stay vigilant about data privacy, especially in the context of your reproductive health. Just as you would protect your wallet or valuable objects, so too should you protect your data!

Until our governments enact meaningful, comprehensive privacy policies that protect all citizens of the digital world, it's up to us to protect ourselves.

In this guide, we offer seven tips to help you do just that.

01 BE CAREFUL ABOUT WHO YOU SHARE YOUR DATA WITH.



One of the most effective measures you can take to protect your data is to be thoughtful about who you're communicating with and how.

In a now infamous case from Nebraska, Facebook messages became evidence in an abortion-related prosecution. Law enforcement obtained a search warrant for those messages acting on a tip they received from a friend of the accused stating that she had seen her take medication intended to cause a miscarriage.

Even if you use an end-to-end encrypted messaging service, or a second phone number, to communicate with a friend or relative, the recipient can screenshot or record those conversations and subsequently report them.

Data privacy is a team sport; it's up to you to choose your teammates wisely and make sure you all agree on privacy measures to keep each other safe.

02 SELECT YOUR PERIOD TRACKING APP CAREFULLY, IF YOU USE ONE.

It has become common for many people to use apps to help track their periods.

These apps are useful in charting the details of your cycle and offer helpful insights into your body. However, the use of the apps may affect your reproductive data privacy. **So choose your period tracker app carefully, consider the data that you're sharing, and do not give more than what is required.**

When choosing a period tracker app, you should look into the app's history and reputation with data sharing, its privacy policy and where the data is stored.

For example, one of the more popular tracking apps, Flo, recently has been a part of a proposed legal settlement that requires the app to share its privacy practices and get users' consent before sharing their health information. This is because Flo disclosed users' health information to third parties with no limits on the use of that data.

It's important to note that the use of period tracking apps can be considerably more risky for those that have increased legal risk factors, such as those who received an abortion and may face criminal charges, because the data retained by these apps could become evidence in prosecutions.

In short...

→ If you like using period tracker apps, as many do, consider switching to an app that has a reputation for being private-by-design, like **Euki** or **Drip**.

→ Additionally, limit the information you share with your period tracker app, and consider the situation you are in, like which state you live in, to help you make an informed decision on whether or not to use an app.

03 REVIEW (AND RESET) THE PRIVACY SETTINGS ON YOUR SMARTPHONE.

You have a lot of different applications on your phone, and they all collect different types of data.

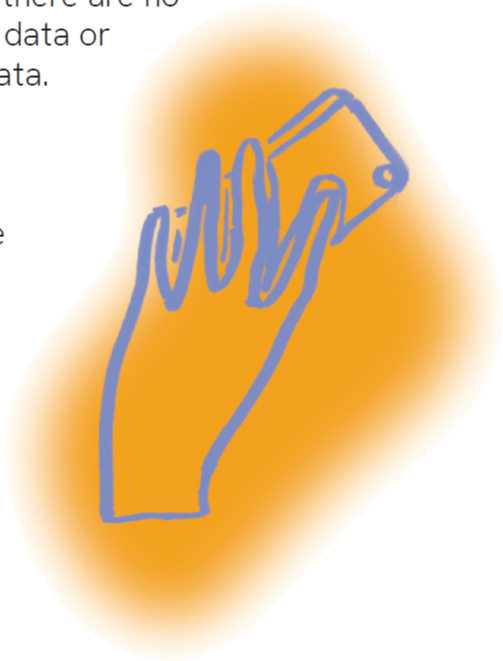
When you download an app, you consent into its End User License Agreement (EULA). These EULA contracts are full of lengthy legal terms, but the common thing they all likely share is you consenting to give the app permission to collect, generate, store, distribute, and sell all data that you share on it.

Because of that, **it is vitally important to visit the privacy menu on your phone and restrict data permissions for individual apps.** Location data is particularly important when visiting an out-of-state clinic which provides reproductive health services.

Follow the instructions below to limit the data you share with apps:

Apple/iOS

→ Go to the "Settings" application and scroll down to select "Privacy & Security."
→ Select the "Location Services" tab and ensure that you are not sharing your location with applications for which it isn't necessary.
→ Then go back to "Privacy & Security" and select the "Tracking" tab and ensure there are no applications tracking your data or requesting to track your data.



Android

→ Find and hold down on the "application" icon on your phone's home screen.
→ Select "App info," then "Permissions," then "Location."
→ Select "App info," then "Permissions," then "Location."

→ There are several different options for location sharing. The safest option is “deny,” which means the application cannot use your location, even while you are using the app. Make sure you select “deny” for all applications which do not need your location data.
→ You can also see the current location app permissions for all of your apps by finding and then selecting “Settings,” then “Location,” then “App Permissions.”

Note: while you are on the “Location” screen, you can turn off “Location” entirely, for all apps at once, which may be useful but also makes navigation impossible and might prevent you from finding your mislaid phone.

Android doesn’t have a feature where you can disallow third party tracking. However, if you download **DuckDuckGo for Android**, they have a free feature which allows you to block third party trackers in the different applications on your phone. App Tracking Protection through **DuckDuckGo** will also allow you to see which applications are trying to get your data.

→ After downloading the DuckDuckGo application, open “Settings,” and select “App Tracking Protection.”
→ Further onscreen instructions on how to utilize the feature will be provided.

04 TURN OFF AD IDENTIFIERS.

Turning off the Ad Identifiers on your phone is an easy win.

This is something you generally only have to do once, and it restricts all the apps on your phone from sharing your personal information with one another.

If you've ever thought to yourself, "my phone is listening to me" after seeing an ad on one app for a product you searched for on another app, that is actually the work of Ad Identifiers.

These Ad Identifiers allow third party trackers to collect data from a user—for example what you like and post on social media, or what you search on an app—to create a profile of you that highlights your preferences and habits. While some may enjoy the personalized ads they get to see, Ad Identifiers are a tool for tech companies to generate profit off of personal data.

The data footprint that can be developed from these technologies has been and will continue to be useful for law enforcement in abortion-related prosecutions. We recommend that you turn off your Ad Identifiers.

Apple/iOS

→ Go to Settings, Privacy & Security, then scroll down to Apple Advertising
→ Turn off Personalized Ads

Most often apps, when you first open them, will ask you for your permission to track your activity, to which you will press the option "Ask App Not to Track".

For apps you have already been using, you can go to your Settings app, scroll down to Privacy & Security, then Tracking, then turn off "Allow Apps to Request to Track." If you prefer that some apps be able to track you, you may still grant access on an app to app basis.

Android

→ Go to Settings, Privacy, then Ads, and then press "Delete advertising ID" and then tap it again on the next page to confirm. This method is for one of the more modern releases, specifically starting with the Android 12.
→ For users with older versions of the Android, you instead choose the option under "Opt out of Ads Personalization" following the same process to get to this stage. This is the "main switch" to turn off ad identifiers, however, there is a way for you to turn off ad identifiers on an app by app basis, depending on your preference.

05 USE AN ENCRYPTED MESSAGING SERVICE FOR SENSITIVE MESSAGES.

Encryption is at the core of all privacy and security technologies.

When you choose communication technologies that are built with strong encryption, you can be rest assured that this is a good step to keep your data safe. Encrypted data is data that is not readable to a human or a computer. It has to be unlocked with an encryption key, which is stored on your device rather than collected by the host site or application.

The key thing to look for when choosing an encrypted messaging service is "end to end encrypted," meaning that from your device all the way over to the other device of the person you are communicating with, your data is encrypted every step of the way.

Some popular strong end-to-end encrypted apps are:

→ Signal
→ Whisper
→ Telegram
→ Cwtch
→ Keybase

06 USE A BROWSER & SEARCH ENGINE THAT STORE LESS INFORMATION, SUCH AS DUCKDUCKGO, ESPECIALLY FOR SENSITIVE SEARCHES LIKE THOSE INVOLVING REPRODUCTIVE DATA.

Using "incognito mode" on Chrome or clearing your search history can be effective in some circumstances, but not all.

Neither of these options will stop third party trackers from collecting data on your online activity. **All of the trackers that exist online still exist in Chrome's incognito mode.** Chrome also has its own trackers, which it doesn't block in incognito mode.

For a more privacy friendly option, consider downloading **Firefox** (available on Desktop, Android, and iOS) or **DuckDuckGo** (available as a browser on Android and iOS).

DuckDuckGo doesn't track your search history and blocks advertising trackers. In providing the encrypted versions of websites, DuckDuckGo limits your Internet provider's access to your browsing history. It also limits the access of anyone who may be snooping on your WiFi. DuckDuckGo has a mobile browser, a browser extension, and a search engine—all three options offer enhanced privacy protections.

AVOID USING YOUR SCHOOL WIFI, SCHOOL ACCOUNT, OR SCHOOL-ISSUED DEVICE WHEN COMMUNICATING OR SEARCHING FOR SENSITIVE INFORMATION SUCH AS THOSE INVOLVING REPRODUCTIVE RIGHTS.

07

Students should be aware of the increased privacy risks associated with the use of school WiFi, school accounts, and/or school-issued devices.

If you are connected to your school's WiFi network, institutions may be permitted to track and monitor your internet activity. Furthermore, if you are conducting research from an account connected to your school's domain (Google Suite, for example), your search history may be visible to your institution. Finally, if you are using a school-issued device or server, any data produced is likely accessible to your school administrator.

When researching sensitive matters, it's best to avoid using your school WiFi, school account, or school-issued-device.

It can be valuable to look up your school's student data policy, which may include opportunities to opt out of data sharing.

For more information, check out these sources:

https://www.eff.org/deeplinks/2022/05/digital-security-and-privacy-tips-those-involved-abortion-access

https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/

https://ssd.eff.org/playlist/privacy-breakdown-mobile-phones

https://support.google.com/android/answer/6179507

https://spreadprivacy.com/app-tracking-protection-open-beta

https://help.duckduckgo.com/duckduckgo-help-pages/privacy/smarter-encryption

https://www.zdnet.com/article/best-browser-for-privacy

https://digitaldefensefund.org/ddf-artwork-zines/digital-security-for-abortion-and-pregnancy-privacy-poster

https://tosdr.org

This guide was created as part of the Reproductive Data Privacy Initiative by The Ethical Tech Initiative @ The George Washington University Law School.

RESEARCH COMPILED BY:
Maya Arigala
Ashley Gómez
Clare Burgess

DESIGNED BY:
Elspeth Walker | elspethkwalker.com

CONNECT WITH US AT:
https://blogs.gwu.edu/law-eti/