The Washington Post
Democracy Dies in Darkness

Seeking an abortion? Here's how to avoid leaving a digital trail.

Everything you should do to keep your information safe, from incognito browsing to turning off location tracking

By Heather Kelly, Tatum Hunter and Danielle Abril
June 26, 2022 at 9:00 a.m. EDT

Everything you do online is already tracked. That information is about to become even more sensitive if you're seeking an abortion in the United States.

Friday's Supreme Court decision overturning the landmark abortion rights ruling *Roe v. Wade* means 13 states could outlaw abortions within a month, and more could follow.

A Google search for a reproductive health clinic, online order for abortion pills, location ping at a doctor's office and text message about considering ending a pregnancy could all become sources of evidence. People constantly share data about their fertility online, privacy advocates say — even if they don't realize it. Other obvious sources of health data include period-tracking apps and digital check-in forms at hospitals.

"People should not be responsible for doing everything perfectly, when they're in a stressful situation, to protect our own privacy," said India McKinney, director of federal affairs for the privacy advocacy organization Electronic Frontier Foundation. "Privacy is a fundamental human right, and it should be protected in law and statutes."

Here are the basic steps anyone can take to protect personal information when weighing an abortion.

Limit who you tell

Your biggest risk factor is other people. Many cases against people who had abortions start with people they've told who report them to law enforcement, according to Farah Diaz-Tello, senior counsel and legal director for If/When/How, a reproductive justice nonprofit.

"The biggest vector for criminalization is the health-care system," Diaz-Tello said. The group has studied cases against people who've had abortions since 2000 and tracked how the process typically happens.

When someone goes to a health provider with medical issues related to an abortion, medical professionals can report them to the police, who can then seize their phones or computers. With a device in hand, police can just look through the browser and text messages directly

through the browser and text messages directly?

Diaz-Tello recommends being judicious about what information you share in an emergency room or doctor's office. A miscarriage and a self-managed abortion using pills will look identical to most health-care providers and require the same treatment, she said.

Limit who you tell in your own life as well, including friends or family. If you're experiencing intimate partner threats, take these steps to protect your communications and devices.

Chat on a secure, encrypted messaging app

When you do discuss your situation, use private messaging apps that use encryption. Apple's iMessage, Meta's WhatsApp and Signal are all end-to-end encrypted by default, which means messages are obscured from everyone except the sender and receiver.

Signal may be the most secure option. Apple has the key to decrypt iMessages that are backed up using its iCloud service, and law enforcement could ask it to do so. WhatsApp, for its part, leaves room in its privacy policy to share data with Facebook parent company Meta. Depending on what data it shares, that could raise privacy problems.

Protect your devices

Keep in mind that someone with access to your physical device could view your messages, whether or not they're encrypted. Don't turn your phone or laptop over to law enforcement without a warrant, privacy experts advise, and turn off biometric authentication such as Face or Touch ID if you're worried about someone pressuring or forcing you to unlock them. Make sure your phone, tablet and computers all require a passcode or password to use them. Avoid wearing any health-tracking wearables while managing your health.

Browse the internet securely

There are two ways your browsing activity could put you at risk: someone seeing it on your device, and someone obtaining it from tech or ad-tech companies, said Eric Rescorla, chief technology officer at Firefox.

Always use incognito or private browsing mode on your browser to avoid leaving a trail on your own devices. When choosing a browser, go with Safari, Firefox or Brave, which all have robust privacy features. Make sure any options to prevent cross-site tracking are turned on, and instead of Google, use a search engine such as DuckDuckGo or Brave.

To minimize what is recorded about your browsing, use a VPN or Apple's iCloud Private Relay, which acts like a more secure VPN. Avoid using third-party apps for searches. If you want an extra layer of protection, use Tor Browser, a tool for anonymous internet use that cloaks both your identity and your location, Rescorla said.

If you do use Google, make sure you are logged out of your account and that you have turned up the dials on all your privacy settings. Confirm any results for abortion clinics are real and not fake "pregnancy crisis" centers. If it's a Google ad, there should be a small line above the site name that says "Provides abortions" or "Does not provide abortions." The National Abortion Federation has a list of vetted providers on its site.

abortions. The National Abortion Federation has a list of vetted providers on its site.

Turn off location sharing, or leave your phone behind

Some apps collect your location throughout the day and night and share it with third parties including data brokers, who sell that data to whoever wants to pay. To turn off location sharing on an Apple device, go to Settings → Privacy → Location Services and toggle the slider so that it shows gray. (Note that this will make apps that depend on location, such as Uber or maps, stop working.) On an Android device, go to Settings → Location and toggle the switch to "off."

Unfortunately, turning off location sharing won't stop your cell carrier from collecting your location. Jennifer Granick, surveillance and cybersecurity counsel at the American Civil Liberties Union, said a Faraday bag, which blocks electromagnetic fields, could help in cases when a person wants to keep their phone on them but prevent location tracking from service providers.

To truly obscure your location, the best thing to do is leave your phone at home or turn it off completely, McKinney said. You can also use a temporary "burner" phone. Don't add any of your accounts, connect to your home WiFi or turn on Bluetooth, she added.

Maximize your privacy settings

To make sure your phone or social media sites are collecting as little data as possible, lock down your privacy settings. You can find a list of the biggest app and device's options in our Privacy Reset Guide.

Avoid period tracking apps

Trusting any app with sensitive medical information is a risk, especially if it's not covered by HIPAA requirements. Each period-tracking app has different privacy practices, and understanding the nuances can be tricky. A password-protected spreadsheet or paper calendar will serve you better.

If you decide to delete your period-tracking app, consider sending a data-deletion request as well, said Alan Butler, executive director and president of the Electronic Privacy Information Center. Some companies only honor these requests from people in California because of the state's privacy law, but others accept requests from anywhere.

"The state and federal government's power to get data right now is incredibly broad," Butler said. "We haven't seen new limits on access to data from government in decades, which means laws … have gotten weaker as tech has evolved."

Limit where you share health information

Your dentist and even your workout instructor may hand out forms asking whether you're pregnant. If you're not comfortable sharing, say so, and save that conversation for a doctor you trust.

comfortable sharing, say so, and save that conversation for a doctor you trust.

Check-in software at your doctor's office may have privacy holes, The Washington Post has reported. A consent form from check-in software maker Phreesia, for example, gives it permission to use your data for marketing. Select "no" on any data-sharing prompts you see.

Push your health-care and insurance providers on what they do with your information, such as the date of last period or pregnancy status. Where is it recorded and stored, is it encrypted, and how long do they keep it? Look over every document you sign to see whether you're giving up any rights to your information, or whether you're giving permission to share it with other parties.

Be cognizant of physical surveillance technology

In some cases, law enforcement may pull data from license plate readers or facial recognition software systems that have been strategically set up along state borders, said Granick of the ACLU. If you're in need of reproductive services, you may want to consider taking alternate modes of transportation vs. driving your own car, for example.

"People should not give up, even though this is hard and may seem like a lot," Granick said. "People should take advantage of what they can do while pushing the powers that be to do more."