

November 22, 2022

ATTORNEY GENERAL RAOUL JOINS COALITION URGING APPLE TO PROTECT CONSUMERS' REPRODUCTIVE HEALTH INFORMATION

Letter to Apple CEO Highlights Security Gaps in Apps Hosted by Apple

Chicago — Attorney General Kwame Raoul, as part of a coalition of 10 attorneys general, is expressing concerns about reproductive health privacy on Apple's App Store following the U.S. Supreme Court's decision overturning *Roe v. Wade*. Raoul and the attorneys general urged Apple to take practical steps to protect consumers' private reproductive health information.

[In a letter sent](#) to Apple CEO Tim Cook, Raoul and the coalition called on Apple to protect the personal information of individuals seeking or providing abortion care by implementing privacy-enhancing measures to safeguard data collected by apps hosted on Apple's App Store.

"As a result of the Supreme Court's ruling overturning *Roe v. Wade*, millions of Americans now must search for alternative methods of managing their reproductive health or seeking abortion services," Raoul said. "Women have a right to seek reproductive health care online without worrying that their data might be used against them. I urge Apple to take these commonsense steps to protect women's private, reproductive health information."

While Apple has adopted privacy and security measures that are consistent with its stated goals of protecting consumers' privacy, apps hosted in its store may not meet the same standards or implement appropriate protections for this sensitive data. According to the coalition, this gap in Apple's protections threatens the privacy and safety of App Store consumers and runs directly counter to Apple's publicly expressed commitment to protect user data.

The letter cites the demonstrated risk that location history, search history and adjacent health data pose to individuals seeking or providing abortions or other reproductive health care. Raoul and the coalition urge Apple to require app developers to either certify to Apple or affirmatively represent in their privacy policies that they will take the following security measures:

- Delete data not essential for the use of the application, including location history, search history, and any other related data of consumers who may be seeking, accessing or helping to provide reproductive health care.
- Provide clear and conspicuous notices regarding the potential for app store applications to disclose user data related to reproductive health care, and require that applications disclose this information only when required by a valid subpoena, search warrant or court order.
- Require app store applications that collect consumers' reproductive health data or that sync with user health data stored on Apple devices to implement at least the same privacy and security standards as Apple with regard to that data.

Raoul and the attorneys general explain that deleting data related to reproductive health care is the first line of defense to protect consumers who, often unknowingly, leave digital trails of their efforts to obtain or provide reproductive health care. The letter also notes that data retention and sharing is often obscured by vague and unclear privacy policies — making it impossible for consumers to make informed decisions about who to trust with their sensitive information. It is critical for Apple to ensure that apps provide clear and conspicuous notices regarding third-party access to reproductive health data, the letter explains.

At a minimum, Apple should require apps on the app store to meet certain threshold security requirements, such as encryption of biometric and other sensitive health data stored on applications, use of end-to-end encryption when transmitting this data, and compliance with Apple's user opt-out controls. Compliance with these measures should be represented in the privacy policies of app store apps.

The letter also urges Apple to implement a clear process to audit third-party apps' compliance with Apple's privacy and security standards. The letter calls on Apple to conduct periodic audits and remove or refuse to list third-party apps in violation of these standards.

Raoul is joined in signing the letter by the attorneys general of California, Connecticut, the District of Columbia, Massachusetts, North Carolina, New Jersey, Oregon, Vermont and Washington.



State of New Jersey

OFFICE OF THE ATTORNEY GENERAL
DEPARTMENT OF LAW AND PUBLIC SAFETY
DIVISION OF LAW
124 HALSEY STREET
PO BOX 45029
NEWARK, NJ

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

MATTHEW J. PLATKIN
Attorney General

MICHAEL T. G. LONG
Director

November 21, 2022

Tim Cook
Chief Executive Officer
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Re: Reproductive Health Rights on the App Store

Dear Mr. Cook:

The undersigned Attorneys General (“State Attorneys General”) write to express concerns regarding reproductive health privacy on Apple’s App Store (the “App Store”) following the Supreme Court decision in Dobbs v. Jackson Women’s Health Organization and to urge Apple to take steps to protect consumers’ private reproductive health information. Third-party apps available on the App Store collect consumers’ private reproductive health data, which can be weaponized against consumers by law enforcement, private entities, or individuals. This gap in Apple’s protections threatens the privacy and safety of App Store consumers, and runs directly counter to Apple’s publicly expressed commitment to protect user data. The State Attorneys General therefore ask Apple to ensure that the apps on its App Store meet the privacy standards necessary to protect against the misuse of private reproductive health data.

Apple has long promoted privacy as one of its “core values”¹ on both the iOS platform and the App Store.² Apple’s guidelines for App Store developers stress that “[t]he guiding principle of the App Store is simple—we want to provide a safe experience for users to get apps and a great opportunity for all developers to be successful.”³ Part of providing a “safe experience” is requiring

¹ Privacy, Apple, <https://www.apple.com/privacy/> (last visited Oct. 20, 2022).

² App Store Review Guidelines, Apple, <https://developer.apple.com/app-store/review/guidelines/#legal> (last visited Oct. 20, 2022).

³ Id.

that apps on the App Store “implement appropriate security measures.”⁴ Indeed, Apple often avers that the App Store can ensure privacy and security in ways that would not be possible without such measures.⁵ Apple assures consumers that the App Store is an important key to securing their app data.⁶

When it comes to app data related to reproductive health, however, Apple has not done enough. Location history, search history, and adjacent health data (specifically, all information relating to the past, present, or future reproductive or sexual health of an individual) pose a significant risk to individuals seeking or providing abortions, birth control, or other reproductive health care. Accordingly, the State Attorneys General urge Apple to require app developers to either certify to Apple or affirmatively represent in their privacy policies that they will take the following three measures:

1. Delete data not essential for the use of the application, including location history, search history, and any other related data of consumers who may be seeking, accessing, or helping to provide reproductive health care;
2. Provide clear and conspicuous notices regarding the potential for App Store applications to disclose to third parties user data related to reproductive health care, and require that applications do so only when required by a valid subpoena, search warrant, or court order; and
3. For App Store applications that collect consumers’ reproductive health data or that sync with user health data stored on Apple devices, implement at least the same privacy and security standards as Apple with regards to that data.

As discussed further below, these actions will safeguard reproductive health information from being wrongfully exploited by those who would use it to harm patients or providers. Failure to certify compliance with these measures should constitute grounds for removal from the App Store. Consumers cannot trust Apple’s privacy promises if applications on the App Store are not required to take active measures to protect this sensitive health data. Provision of an app or service should not come at the cost of consumers losing control of their health data. To that end, Apple should pursue these measures to protect consumers’ reproductive health privacy. These steps will ensure that Apple stays true to its commitment “to provide a safe experience for users.”

⁴ Id.

⁵ Bree Fowler, Apple’s Tim Cook Says the Fight to Protect Privacy Is a Crucial One, CNET (Apr. 12, 2022 7:29 AM), <https://www.cnet.com/news/privacy/tim-cook-says-the-fight-to-protect-privacy-is-a-crucial-one/>.

⁶ App Store stopped nearly \$1.5 billion in fraudulent transactions in 2021, Apple (June <https://www.apple.com/newsroom/2022/06/app-store-stopped-nearly-one-point-five-billion-in-fraudulent-transactions-in-2021/>).

Deleting Data Related to Reproductive Health Care

Deletion is the first line of defense to protect consumers who, often unknowingly, leave digital trails of their actions to obtain or provide reproductive health care. And while app developers have an independent responsibility to safeguard user data, the financial incentive for collecting a large volume of data runs counter to consumers' expectations of privacy. For example, data brokers may collect and compile reproductive health information from mobile apps, including names, demographic information, contact information, location information, browsing and search history, and other health information. This information is then used to create a comprehensive profile of an individual, and can be aggregated to fit a specific demographic category. For instance, data brokers have sold 2.9 billion profiles of Americans identified as "actively pregnant" and/or "shopping for maternity products" and 478 million customer profiles labeled "interested in pregnancy" or "intending to become pregnant."⁷ The bulk data is then typically sold to either marketing agencies or other data brokers, but it can also be used by law enforcement or private actors to target individuals.

Private purchasers of this sensitive data can use this information to harass, intimidate, or deter individuals who seek or provide reproductive health care. In fact, crisis pregnancy centers, many of which are affiliated with national anti-abortion advocacy groups, purchase this data to target advertisements to individuals under the guise of providing counseling or other health care. As a result, these centers are able to gather even more health data from individuals seeking care at these centers—including sexual and reproductive histories, test results, and ultrasound photos. Crisis pregnancy centers can then use that data to either interfere with individuals' access to abortion care, or disclose the information to law enforcement in states that have re-criminalized abortion.

Requiring apps to proactively delete location, search, and health data of consumers who have researched, sought, or provided reproductive health care—which is not necessary to the purpose of the application—will limit the potential flow of data from apps to those that seek to either exploit such information or punish individuals for seeking to access reproductive care. Ultimately, Apple is the gatekeeper that can condition App Store access upon deletion of users' reproductive health data; the onus should not be on consumers to request deletion. Despite Apple's efforts to protect privacy by requiring app developers to provide information about their app's privacy practices—including on data deletion and user tracking—certain third-party apps have been found to circumvent Apple's privacy requirements and continue to communicate with third-party trackers even after consumers request that these apps not track their data.⁸ Deletion is the

⁷ Shoshana Wodinsky & Kyle Barr, [These Companies Know When You're Pregnant—And They're Not Keeping It Secret](https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426), Gizmodo (July 30, 2022), <https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426>.

⁸ Geoffrey A. Fowler & Tatum Hunter, [When you 'Ask app not to track,' some iPhone apps keep snooping anyway](https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/), The Washington Post (Sept. 23, 2021 6:00 AM), <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/>.

better security measure that significantly limits the amount of data companies collect, store, and share.

Providing Clear and Conspicuous Notices Regarding Third-Party Access to Reproductive Health Data

The data that apps do retain may be subject to requests from law enforcement in states that have passed laws criminalizing abortion. Law enforcement may use reproductive health data obtained from apps to prosecute individuals—even those who do not ultimately terminate their pregnancies. For example, in 2017, a Mississippi woman named Latice Fisher gave birth to a stillborn baby.⁹ Law enforcement found that she had conducted an online search for abortion pills. Even though there was no evidence Fisher had actually taken the pills, the online search history was used as evidence in the murder case against her. Similarly, in a 2015 Indiana case, Purvi Patel became the first woman in the United States to be charged, convicted, and sentenced for feticide for terminating her own pregnancy. The state prosecutor’s evidence included texts, web browsing history—including a visit to a webpage titled “National Abortion Federation: Abortion after Twelve Weeks,”—as well as an email from a website that provided mifepristone and misoprostol (abortion-inducing medication) without a prescription. Although the conviction was later overturned, this case reflects the rise in the use of search history data and other user data to build cases against individuals seeking to terminate a pregnancy.

Many apps that collect reproductive health data use boilerplate statements that do not clearly identify the conditions under which the app shares data with law enforcement.¹⁰ Consumers who are not appropriately apprised of the potential for their interactions with an app to be documented and produced to others—including law enforcement—are thus unable to provide informed consent for the apps’ collection and sharing of their information. This is especially true of younger individuals who have little experience understanding and navigating the complex data collection and sharing economy.

Moreover, consumers have made it clear that they are deeply concerned about apps’ murky privacy practices post-Dobbs. For instance, Flo Health, the popular period-tracking app, was found to be misrepresenting its data collection and sharing practices even after a 2021 FTC settlement. That settlement required Flo “to obtain the affirmative consent of users of the company’s fertility-tracking app before sharing their personal health information with others and

⁹ Cat Zakrzewski, Pranshu Verma & Claire Parker, Texts, web searches about abortion have been used to prosecute women, The Washington Post (July 3, 2022, 9:20 AM), <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/>.

¹⁰ In Post Roe v. Wade Era, Mozilla Labels 18 of 25 Popular Period and Pregnancy Tracking Tech With *Privacy Not Included Warning, Mozilla Foundation (Aug. 17, 2022), <https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/>.

to obtain an independent review of their privacy practices.”¹¹ Once the settlement became public, Flo’s user rates steadily declined until Flo implemented an “anonymous mode” that would allow users to use the app without attaching their name, email, or other technical identifiers to their health data.¹² But the inconsistency across reproductive health apps nevertheless has left consumers confused as to which apps will safeguard their information, and, as a result, consumers are forced to choose between apps that are equally concerning on the privacy front.¹³ Accurate disclosures to consumers would rectify this issue.

Short of deleting reproductive health data altogether—which is the preferred solution—apps must provide users with an explanation of how and what types, if any, of their sensitive information is collected, retained, used, and shared. To that end, app developers must clearly and conspicuously notify users if and under what circumstances the apps will disclose reproductive health data to law enforcement and others. These required disclosures should not be hidden in lengthy, unclear policies that vary from app to app. Users should be fully informed of the potential for their data to be turned over to third parties, and be able to make decisions about their app usage accordingly. Requiring such disclosures about such sensitive information should be a condition precedent to the apps’ availability on the App store.

Ensuring Apps that Collect Reproductive Health Data and that Sync with Apple Health Data Comply with Apple’s Existing Privacy and Security Standards

Apple has adopted a number of privacy and security measures that are consistent with its stated goals of protecting consumers’ privacy. For example, Apple ensures that Apple Health data—including reproductive data—is automatically encrypted.¹⁴ Apple also provides privacy controls that allow consumers to limit the application’s access to certain sensitive information¹⁵

¹¹ Flo Ovulation & Period Tracker, Mozilla Foundation (Aug. 9, 2022), <https://foundation.mozilla.org/en/privacynotincluded/flo-ovulation-period-tracker/>; FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, Federal Trade Commission (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

¹² Rebecca Pifer, Period tracker Flo launches anonymous mode amid post-Roe privacy concerns, Healthcare Dive (Sept. 15, 2022), <https://www.healthcaredive.com/news/flo-anonymous-mode-period-tracker-app-abortion-roe/631926/>.

¹³ Sarah Perez, Consumers swap period tracking apps in search of increased privacy following Roe v. Wade ruling, TechCrunch (June 27, 2022 3:36 PM), <https://techcrunch.com/2022/06/27/consumers-swap-period-tracking-apps-in-search-of-increased-privacy-following-roe-v-wade-ruling/>.

¹⁴ iOS Health, Apple (last visited Oct. 20, 2022), <https://www.apple.com/ios/health/>.

¹⁵ App privacy details on the App Store, Apple Developer (last visited Oct. 13, 2022),

and requires apps to request permissions only when needed to provide the service.¹⁶ However, third-party apps that sync with Apple Health, as well as apps that independently collect reproductive health data from consumers, frequently fail to meet these same standards.¹⁷

For example, Mozilla Foundation recently surveyed popular reproductive health apps and applied “Privacy Not Included” warnings to the worst offenders.¹⁸ It evaluated how each company uses, shares, sells and retains the data it collects, as well as the security measures employed by the app.¹⁹ Of the twenty-five reproductive health apps surveyed by Mozilla Foundation—including period tracking apps, pregnancy/fertility apps, and health/fitness wearable devices—the majority (eighteen apps) either failed to abide by proper privacy and security practices, or obfuscated the scope of user data collected by the apps.²⁰ Many apps failed to meet minimum security standards such as use of encryption, automatic security updates, strong password requirements, and a clear and accessible privacy policy. Some apps lacked even basic privacy policies, let alone policies that addressed the use of sensitive information. A majority of apps surveyed also prompted consumers to input information outside of the scope of the health services offered by the app. Taken as a whole, the majority of these reproductive health apps did not meet accepted security standards and fell far short of consumers’ expectations of privacy.

The number of health apps with substandard security practices is deeply concerning as it leaves reproductive health data vulnerable to compromise and misuse—a fact Apple understands given the security measures it has already implemented. Given that understanding and Apple’s consistent promotion of its commitment to privacy, consumers reasonably expect the same from the third-party apps that Apple allows on the App Store. But although Apple reviews all apps for compliance with developer guidelines prior to their launch on the App Store, apps continue to find ways to circumvent those requirements. Certain apps change their policies after receiving approval to be offered on the App Store, while others ignore those commitments entirely.²¹

To remedy these issues, Apple must implement a clear process to audit third-party apps’

<https://developer.apple.com/app-store/app-privacy-details/#additional-guidance>.

¹⁶ User Privacy and Data Use, Apple Developer (last visited Oct. 20, 2022), <https://developer.apple.com/app-store/user-privacy-and-data-use/>.

¹⁷ See Fowler, *supra* n. 8.

¹⁸ See Mozilla Foundation, *supra* n. 10.

¹⁹ Id.

²⁰ Id.

²¹ See Fowler, *supra* n. 8.

compliance with Apple’s privacy and security standards.²² At minimum, Apple should require apps on the App Store to meet certain threshold security requirements, such as encryption of biometric and other sensitive health data stored on applications, use of end-to-end encryption when transmitting said data, and compliance with Apple’s user opt-out controls. Compliance with these measures should be represented in the privacy policies of App Store apps. To ensure long-term compliance, Apple should conduct periodic audits and remove or refuse to list third-party apps in violation of these standards. These reviews should also occur any time a new privacy policy is adopted by the app. Apple should not condone the presence of third-party apps on the App Store that fail to maintain the same level of privacy and security as itself to safeguard reproductive health data.

Conclusion

We acknowledge Apple’s commitment to privacy and security across its products, as evidenced by its use of encryption to protect user health data as well as its transparency into law enforcement requests for user data. But that alone is insufficient if third-party apps on the App Store fail to respect and adhere to Apple’s privacy ethos. The millions of consumers who use Apple’s App Store to obtain health and reproductive services rely on Apple’s assurances of privacy. We urge Apple to honor its commitment to protecting consumer privacy by requiring the apps hosted on its platform to do the same.

Sincerely,



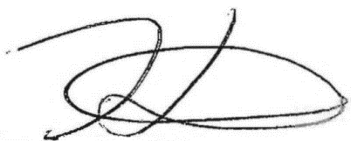
MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY



Rob Bonta
California Attorney General



William Tong
Attorney General of Connecticut



Karl A. Racine
District of Columbia Attorney General



Kwame Raoul
Illinois Attorney General

²² Id. (“Without thorough audits, it may be hard even for Apple to know exactly what happens to data after it leaves an app and goes to a third party...Apple’s enforcement has dried up, and data companies are seeing how far they can push it.”)



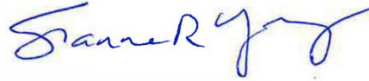
Maura Healey
Attorney General of Massachusetts



Josh Stein
Attorney General of North Carolina



Ellen Rosenblum
Attorney General of Oregon



Susanne R. Young
Vermont Attorney General



Bob Ferguson
Washington State Attorney General