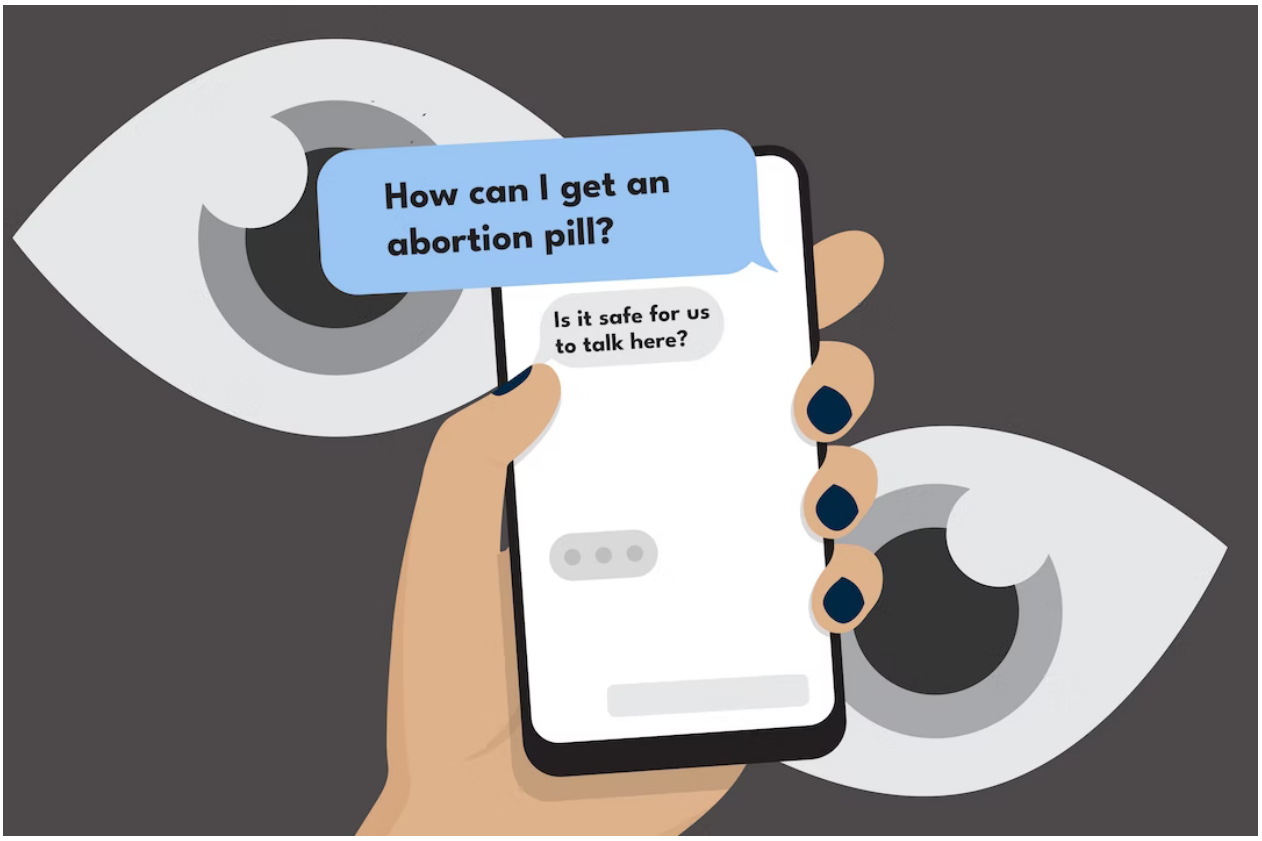
THIRD WAY

MEMO *Published January 22, 2023 • 23 minute read*

The New Front in the Battle for Digital Privacy Post-Dobbs



Mike Sexton
Senior Policy Advisor for Cyber
@MikeESexton

Takeaways

The *Dobbs* decision to overturn *Roe v. Wade* is exposing Americans to unprecedented intrusions into their private decisions and activities. Our purchases, communications, travels, health information, and innermost thoughts are logged, stored, and transmitted at a scale unimaginable half a century ago. As some federal and state lawmakers move to criminalize abortion care, the evidence available to investigate and prosecute abortion in 2023 towers over what could have been collected in 1973.

- Period-tracking apps: law enforcement exposure could depend on where the app company's headquarters is located.

- Chats and Message apps: private conversations could be outed if encryption is not end-to-end.
- State privacy law: California's new law guarding digital privacy will likely be challenged in court in other states and doesn't apply to cell phone companies not headquartered in the state.
- GPS: Physical tracking devices could provide a roadmap to prosecution.

With the protection of *Roe v. Wade* rescinded and an emboldened effort to criminalize both patients and providers of abortion care, the private chats, searches, and other pieces of our daily digital footprint are suddenly the epicenter of a new the battle for privacy. Unshackled by the Supreme Court's *Dobbs* decision, anti-choice lawmakers are pursuing legislation to prosecute women and those who care for them, made possible by the technology and data used in our everyday activities and communications. With estimates that one in four women will have an abortion, [1] a significant number of Americans may find that private medical decisions, conversations, and personal data now expose them to criminal liability.

Post-*Dobbs*, there are myriad avenues that law enforcement could potentially exploit to prosecute women seeking an abortion – leveraging a digital trail that few women would reasonably expect could be used against them.

Law enforcement agencies generally obtain an individual's data in one of three ways: by accessing the physical device, making legal requests to tech companies, or buying the data from a third party.

In this paper, we outline the major ways *Dobbs* is rippling through the technology sector, impacting tools and apps that are used every day by millions of Americans. Keeping pace legislatively with these rapid changes in a sector that is already highly fluid will be daunting, but the fate of millions of women who need an abortion, as well as the medical professionals who provide abortion services, hang in the balance.

Period-Tracking Apps

One of the first alarms raised in the immediate aftermath of *Dobbs* was how period-tracking apps could be weaponized by law enforcement in states with abortion prohibition to identify and punish women having abortions. Period-tracking apps are often used to help discreetly plan around menstrual cycles, identify when one is most fertile, or notice any irregularities that may be indicative of an underlying health issue. [2] Many worry a prolonged missed period followed later by a return to a normal menstrual cycle could tip off police to an aborted pregnancy – a hypothetical that sounds like it originated in *The Handmaid's Tale.*

How a period app may be leveraged by law enforcement depends on where the app developer is headquartered, where users' data is stored, and whether the data is sold to any third parties such as data brokers. [3] For example, the popular period app Clue is based in Germany, where it is prohibited under EU law from sharing users' health data – including to advertisers or law enforcement the United States. [4] The astrology-oriented period tracker Stardust went viral in the immediate aftermath of *Dobbs* for its allegedly strong privacy protections, but has turned out to have more ambiguous policies and technological protections in place for users. [5]

A data broker is a company that collects and aggregates user information from other companies, like location history, purchases, contact details, and social media profiles. Data brokers can help companies tailor better products and advertisements, but their secrecy and lack of regulation raise serious privacy concerns. Data brokers generally do not have a direct relationship with the consumers whose data they store.

Another highly popular period tracker Flo settled Federal Trade Commission allegations in 2021 [6] [7] that the company shared its users' health data with third-party data analytics providers despite promising such data would be kept private and despite the third parties' terms prohibiting the sharing of such data. [8] In a case where a period app has shared a user's menstrual data, the police could seek such data either from the app itself or any third parties it disclosed such information to. (Flo, to its credit, has become a privacy innovator since *Dobbs v. Jackson,* rolling out a new "Anonymous Mode" [9] that allows users to track their menstrual information without logging any identifying information, and, under its FTC settlement, is prohibited from sharing users' health data with third parties without consent.) Even after a user has deleted a period-tracking application, the application may still hold onto their data [10] unless requested to delete it. Altogether, someone who has procured or self-induced an abortion while living in a state where it is illegal would be justified in feeling paranoid about how any period-tracking apps they have used may, in turn, be used against them.

How a period app may be leveraged by law enforcement depends on where the app developer is headquartered, where users' data is stored, and whether the data is sold to any third parties such as data brokers.

Some experts, however, are less concerned about the legal risk that period-trackers could pose to women seeking abortions. As Kendra Albert (Harvard Cyberlaw Clinic), Maggie Delano (Swarthmore College), and Emma Weil (Upturn) point out, no digital evidence-based prosecutions of

abortion [11] anywhere in the world have relied upon data from period tracking apps. Because a self-induced abortion and a miscarriage are medically indistinguishable and would show the same effect in someone's menstrual cycle, it would be difficult to prove intent in such a case without something more substantive, like search history or messages (which have been used in such prosecutions and are discussed below).

Chat Applications and Encryption

One police investigation in Nebraska reported shortly after the *Dobbs* decision spurred a notable amount of debate and uproar – as well as misinformation and misunderstanding. In June 2022, Nebraska police issued Meta a warrant for the Facebook Messenger private messages of a 17-year-old and her mother after police had exhumed a fetus that had been buried in a plastic bag. [12] The family told the police detective that the 17-year-old had given birth prematurely to a stillborn child, and then buried it themselves. Because the fetus was in a plastic bag, police sought the mother and daughter's Facebook messages to determine if it was truly stillborn or had been asphyxiated. The turned-over messages showed that the daughter self-induced an abortion with her mother's help while 28 weeks pregnant.

Hereafter, many misconceptions abounded. Nebraska police issued the warrant to determine whether the baby had been stillborn or asphyxiated – not aborted – and Meta was not provided any details in the warrant regarding the basis of the investigation. Furthermore, while the news reporting took place after *Dobbs,* the events themselves occurred *before* the Supreme Court decision. Finally, none of the charges levied against the family hinged on *Dobbs* – the abortion was terminated at 28 weeks, outside Nebraska's 20-week window pre-*Dobbs*, and was not performed by a physician, as state law required.

Nevertheless, the furor prompted important questions about how Facebook Messenger and other chat applications would handle law enforcement requests post-*Dobbs.* This controversy would likely have been prevented if the mother and daughter had been using end-to-end encryption. When encryption is "end-to-end," it means that the content of the message (or video, call, or file) is encrypted at every point between the sender and receiver. No unencrypted, readable records of the communication ever transit through or get stored at the intermediary – in this case, Meta.

For example, Meta owns another chat application WhatsApp whose messages are end-to-end encrypted by default. [13] If police had issued Meta a warrant for WhatsApp chats instead, they would have only received undecipherable gibberish unless they could unlock one of the investigation targets' devices.

Facebook first offered an encrypted option on Messenger in 2016, [14] but very few users have changed their settings to enable it. This may be due to the general public's low level of knowledge and understanding of the option. Meta's research has found that users quickly become confused

when asked about encryption and instead become concerned that Meta was reading their messages up until now.

A sudden shift to widespread end-to-end encryption also faces a number of challenges. Users prioritize being able to access their prior messages over the messages' privacy. That accessibility could be impeded if their chats are all encrypted and locked behind passwords wholesale across devices. Built-in end-to-end encryption would also make a chat app more difficult for users with limited data storage and bandwidth, and it would cut off communications between users unless all parties in a chat have updated Messenger to enable encryption.

Facebook first offered an encrypted option on Messenger in 2016, but very few users have changed their settings to enable it. This may be due to the general public's low level of knowledge and understanding of the option.

TWEET THIS

The overturn of *Roe v. Wade* will likely reignite tech companies' motivation to roll out encryption for customers and users by default – a trend that began soon after the leaks of Edward Snowden. Meta and similar companies can render any evidence police may seek useless and avoid controversy simply by encrypting all user chats by default. Rolling out strong encryption more widely is a good thing – encryption is a net-positive for Americans individually and as a nation [15] – but it does have tradeoffs: strong encryption makes law enforcement and intelligence investigations more difficult, no matter how high the stakes are. Conflicts between cops and Silicon Valley like the infamous 2016 legal standoff between Apple and the FBI [16] over the San Bernardino shooter's iPhone will become more likely. Police and intelligence agencies will have to be more creative and resourceful about navigating around encryption to achieve access to plaintext evidence [17] (as, in fact, they did in the San Bernardino case). [18]

California Data Haven

On September 27, California Governor Gavin Newsom signed AB 1242: [19] a bill to make the state a "data haven" for health information related to abortion and reproductive health. The bill requires that outside law enforcement show the information they seek from a California corporation is not related to any abortion-related crime [20] that would be legal under California's own laws. It bans California police from sharing information about abortion with police outside the state and largely stops tech companies in California from sharing information related to abortion with outside investigators.

Tech companies like Google and Meta, under AB 1242, are restricted from providing GPS data, user searches, personal communications, or any other data if issued with an out-of-state warrant for an abortion investigation. This applies not only for abortions performed in California, but anywhere, as long as the data sought is held by a California company. Given that American technology giants are overwhelmingly headquartered in California, the implications of this legislation are vast.

But GPS data is not the only way to track a suspect's location. When a cell phone connects to the nearest cell tower, the tower logs the device's connection and approximate location. In urban areas where cell towers are closer together, this data can be used to triangulate a person's location as closely as ¾ of a square mile. [21] This is much less precise than GPS data, but taken together with other data, such a period app, may suffice to show a suspect traveled out of state to procure an abortion.

No mobile service providers in the US are headquartered in California, meaning cellular triangulation data is not clearly protected under AB 1242. If a police department in an abortion-prohibiting state parleys directly with the mobile service provider, circumventing California police, it is possible they may even be able to prosecute an abortion performed *within California.*

Besides the cellular triangulation loophole, the sweeping data protections in AB 1242 are likely to be challenged in federal court. These companies frequently have not only customers but offices across the country, including the states in question. While proponents of AB 1242 believe the measure is eminently justified, they are not necessarily optimistic [22] that it will stand up to judicial scrutiny.

If a police department in an abortion-prohibiting state parleys directly with the mobile service provider, circumventing California police, it is possible they may even be able to prosecute an abortion performed within California.

It is also important to note that this legislation would not have prevented Nebraska police from obtaining evidence from Meta in the aforementioned abortion investigation. [23] In that case, Nebraska police requested a warrant to investigate the asphyxiation, burning, and illegal burying of an infant. That may portend future, bad-faith manipulation of search warrants for infanticide or illegal burying of a body that are, in fact, pursuant to an abortion case, but it is much too early to tell.

Abortion Clinics and GPS

With abortion criminalized, Planned Parenthood and other clinics offering abortions will become the legal equivalent of trap houses, with one key difference: trap houses don't publicly list their addresses.

To demonstrate the risk that GPS data could pose post-*Roe,* a Vice investigative reporter purchased location data from the third-party data broker company SafeGraph, [24] which aggregates GPS data collected from other smartphone apps. Its datasets have many mundane and even noble use cases, such as tracking customers' visits to Dunkin' vs. Starbucks to determine brand loyalty, or even identifying super-spreader events in a pandemic. However, post-*Dobbs* their GPS data at abortion clinics can be quickly weaponized at scale.

The GPS data for one week of visits to over 600 Planned Parenthood facilities nationwide cost only $160 to acquire. Although the data does not include the identities of the visitors, it gives informed guesses of where they live based upon where smartphones tend to spend the night, broken down by census tract. Datasets like this can quickly be seized upon not only by law enforcement to punish people having abortions, but also by anti-abortion vigilantes seeking to "doxx" [25] and harass patients. Anti-abortion activists already use location data to target anti-choice ads [26] at phones in abortion clinics. SafeGraph has since committed to stop selling location data of people visiting abortion facilities. [27]

The GPS data for one week of visits to over 600 Planned Parenthood facilities nationwide cost only $160 to acquire.

TWEET THIS

For years, researchers have known and demonstrated [28] the privacy risks of tracked location data, even when it is anonymized. This issue long predates *Dobbs* and far exceeds it in scope. Foreign intelligence agencies, for example, could quickly winnow targets for blackmail by narrowing a dataset of smartphones in DC to those that spend working hours in the Capitol Building and recently spent a few days in a psychiatric or drug rehabilitation facility. Last year, a Catholic publication purchased location data from the popular gay hook up app Grindr to out a priest [29] whose GPS coordinates included gay bars, the U.S. bishops conference headquarters, and his personal residences – leading him to resign.

Even without data brokers, companies like Google are often asked for this location data directly in so-called "geofence" warrants, [30] requesting information on who visited a particular location such as a crime scene in a certain period of time. Google requires users to opt into collecting their personal location data instead of collecting it by default. Google's policy also includes multiple layers of safeguards against overbroad geofence searches in investigations, such as initially

anonymizing the data that is shared. However, Google will de-anonymize certain data, allowing police to identify whose phones were at the place in question, if law enforcement can produce enough information that affirms the need.

Although these warrants are incredibly useful for investigators, their use raises serious privacy concerns. [31] Depending on the location and timeframe, these warrants have the potential to identify hundreds of people, possibly contravening the Fourth Amendment protection against unreasonable searches and seizures. One federal judge in Virginia has ruled that the high number of innocent bystanders swept up in a geofence warrant makes them unconstitutional, [32] although this does not affect the legality of geofence warrants elsewhere in the country.

In response, Google announced in July that it will significantly curtail [33] its user data tracking, even when customers opt in. Location data for visits to domestic violence shelters, abortion clinics, addiction treatment facilities, and other similar places will no longer be stored. The company will also be more reticent in complying with law enforcement requests for data, hopefully protecting users who are getting abortions at illicit facilities in states with abortion prohibition. (Apple does not store user location data.)

Search Engines and Healthcare

Search engines like Google (and Google Maps) have previously come under scrutiny in the abortion debate, but for a very different reason: for years, anti-abortion activists have eagerly bought up ad space and stood up *anti*-abortion clinics – usually termed "crisis pregnancy centers" – in order to bait-and-switch people seeking abortions. According to a June 2022 letter by Senator Mark Warner (D-VA) and Congresswoman Elissa Slotkin (D-MI), [34] 37% of Google Maps and 11% of Google search results for "abortion pill" and "abortion clinic near me" turn up anti-abortion clinics, in select states. 28% of Google ads were also for anti-abortion clinics. Google has since begun clearly labeling and distinguishing between facilities that actually perform abortions and anti-abortion clinics, [35] so that a user searching for nearby abortion clinics will no longer have "crisis pregnancy centers" misleadingly displayed.

One way law enforcement could investigate abortion would be by serving Google with a warrant or subpoena for anyone who performed a particular incriminating search, like "how to induce an abortion." In this hypothetical, investigators begin with the *search query* and then use *that* to identify users – they do not begin with a suspect and then check their search history (which is commonplace and largely uncontroversial). This technique, which some consider an unconstitutional search and seizure under the Fourth Amendment, is known as a "keyword search" or "reverse keyword search." Privacy activist Albert Fox Cahn likens this to asking a library to share the names of anyone who checked out a specific book, saying "we would never allow that in the analog world." [36] Depending on how narrow the parameters of a keyword search are, it could be characterized as a "fishing expedition" [37] – an informal, subjective legal term for an overbroad search for incriminating information by investigators.

The constitutionality of keyword searches may become clear sooner rather than later. In Denver, police investigating an arson that killed five members of a Senegalese immigrant family asked Google to identify any users [38] who had searched for the address of the home in the 15 days before it was attacked. After initially pushing back, Google returned information on 61 search queries. Investigators winnowed down those results, asking Google for more information on the ones that looked promising. Police eventually homed in on one 17-year-old and issued requests to Meta, Snapchat, and cell carriers for more detail on his other online activities and communications, eventually collecting enough evidence to charge him and two other juveniles. Lawyers for the teenage defendant argue that the original keyword search that first led police to him and his alleged accomplices was unconstitutional – the first defense team ever to legally challenge this technique in court.

If keyword searches withstand judicial scrutiny under the Fourth Amendment, the implications for abortion prohibition are serious, but we must right-size our concerns. The propriety of keyword searches, if they are judged to be constitutional, will likely depend on how narrowly the investigators are searching. Police cannot, under the Fourth Amendment, keep a running list of everyone who borrows *The Anarchist Cookbook* from the local library. However, if someone detonates a bomb matching the exact specifications in *The Anarchist Cookbook,* a judge will likely approve a law enforcement warrant requesting records of who recently borrowed it from the library. Similarly, a judge is unlikely to grant a perpetual warrant for anyone searching "where to get an abortion nearby" in a state with prohibition, but they may grant one in a limited timeframe and geographic area if police bust an illicit abortion facility.

If keyword searches withstand judicial scrutiny under the Fourth Amendment, the implications for abortion prohibition are serious.

Keyword searches are distinct from a more traditional investigation of a specific user's search history. If law enforcement officials have good reason to suspect someone of a serious crime, they have wide latitude to investigate that person's activity online and offline – whether that crime is arson or abortion. So it is important to differentiate between police asking Google "who is searching for how to get an abortion?" and "did this suspect in particular search for how to get an abortion?"

In August 2022, several hundred Google employees signed a petition [39] asking the company to protect users, employees, and contractors in several ways regarding abortion post-*Dobbs*, including refusing to comply with law enforcement demands for abortion-related searches. While Google's July announcement [40] broke ground in privacy policy by declaring the company would

systematically purge records of visits to abortion clinics and similarly sensitive facilities, it did not explicitly say it would deny abortion-related search requests – rather, it affirmed its longstanding policy of pushing back on requests it considers "improper" or "overly broad." Now that California Governor Gavin Newsom has signed AB 1242, Google no longer has discretion to comply with or deny out-of-state legal demands for abortion-related searches: as long as the procedure is legal in California, Google will be prohibited from complying with the request.

Criminalizing Providing Info on Abortion

Since *Dobbs*, there has also been a push for "aid and abet" laws that would further criminalize a broad swath of health care providers, family members, or friends even tangentially related to an abortion. In July 2022, three Republican South Carolina state senators introduced a sweeping bill to criminalize abortion, [41] known as SB 1373 or the "Equal Protection at Conception – No Exceptions – Act." The bill features the classics of anti-abortion extremism: up to 25 years in prison for anyone performing or procuring an abortion, with no exceptions for rape or incest. But one specific subsection has raised eyebrows: SB 1373 would make it illegal to "aid, abet, or conspire" to provide an abortion, including "providing information… by telephone [or] internet" and "hosting or maintaining an internet website" if the perpetrator knows "the information will be used, or is reasonably likely to be used."

SB 1373 faced swift and sweeping opposition from the Electronic Frontier Foundation, [42] Center for Democracy & Technology, [43] and several other technology- and human rights-focused advocacy organizations. Even South Carolina's Republican Governor and State Senate Majority Leader have opposed the bill, [44] due to First Amendment violations. The State House of Representatives instead passed the narrower HB 5399, [45] criminalizing abortion with exceptions for rape and incest, and no mention of criminalizing merely providing information. Currently, SB 1373 looks doomed, but as unhinged as it may be, it is not entirely an outlier: the bill is based on model legislation by the National Right to Life Committee (NRLC), the oldest and largest anti-abortion organization in the country.

SB 1373 would make it illegal to "aid, abet, or conspire" to provide an abortion, including "providing information… by telephone [or] internet" and "hosting or maintaining an internet website" if the perpetrator knows "the information will be used, or is reasonably likely to be used."

TWEET THIS

The ramifications of SB 1373 for the First Amendment are clear to observers across the political spectrum. They are also absurd. The aforementioned 1971 *Anarchist Cookbook* remains in circulation today, indexed by the Library of Congress, [46] despite containing literal instructions to build explosives and manufacture LSD, having survived countless concerned letters [47] from Americans to J. Edgar Hoover's FBI, under the aegis of President Richard Nixon. If *The Anarchist Cookbook* is protected under the First Amendment, it is hard to imagine a website offering information on how to access abortion services is not. Criminalizing the provision of information to procure or induce an abortion is simply unconscionable, unconstitutional, and unworkable.

Oklahoma has passed a similar but vaguer law, [48] which is being called the strictest in the country. The Oklahoma statue makes it a felony to "advise" anyone or provide them means to procure an abortion. That, arguably, covers the same ground as South Carolina's bill and beyond, creating possible criminal liability not only for online information providers but confidantes, rideshare drivers, librarians, and even employers who cover reproductive healthcare and travel costs for employees who must leave the state to undergo an abortion. Medical practitioners in the state worry they will face criminal penalties for merely telling a patient what their options are.

Given the vague and broad nature of the Oklahoma law's phrasing, it is deeply chilling for Oklahomans' privacy, freedom of speech, and access to reproductive medicine. Yet, for the same reason, it remains to be seen what exactly it will mean for digital freedom and online privacy in practice. Perhaps prosecutors will focus on parties that arguably "aid and abet" an abortion in a narrow and material sense, such as employers that offer to cover the costs for any staff that must travel out of the state for an abortion (an example Oklahoma Senate President Pro Tempore Greg Treat cites). While ghoulish, exercising that discretion may minimize the law's impact on digital privacy and rights – both in Oklahoma and any other state that chooses to emulate it.

The state of California has forcefully pushed back against legislative efforts like those in Oklahoma and South Carolina by launching abortion.ca.gov, a resource for Americans both inside and outside California to learn more about abortion, their rights, providers, and reproductive care financing. The website, which collects no personal information on visitors, is available in English and Spanish and will be translated into more languages. Other states may seek to suppress this information by blocking their citizens from accessing the website, but efforts like this generally fail without an authoritarian apparatus of surveillance and censorship on par with that of the Chinese Communist Party.

Conclusion

Since the landmark Supreme Court decision *Dobbs v. Jackson Women's Health Organization* was decided in June 2022, overturning nearly five decades of precedent set by *Roe v. Wade*, the ramifications for American society have been staggering and far-reaching. What was once a medical procedure, protected by a constitutional right to privacy, is now a serious crime punishable by up to five, 10, or even 15 years in prison.

The impacts of this tectonic shift in the internet and technology space are still becoming apparent. *Roe v. Wade* held that the "liberty" in the Fourteenth Amendment constitutionally protected the right to individual privacy, which is also a core principle in how modern communications technologies are designed. [49] Stripping this constitutional right and reclassifying it as a crime will affect digital technology profoundly and gravely. Technology executives and state governments are being forced to deal with this ugly reality, whether they support it or not. Policymakers will need to step in.

TOPICS

CYBERSECURITY 101 | ABORTION/CONTRACEPTION 80

ENDNOTES

1. Sanger-katz, Margot, et al. "Who Gets Abortions in America?" The New York Times, The New York Times, 14 Dec. 2021, https://www.nytimes.com/interactive/2021/12/14/upshot/who-gets-abortions-in-america.html.

2. Sarah Bradley, et al. "These Period-Tracking Apps Are the Best and Safest Ones to Use Right Now." Women's Health, 26 July 2022, https://www.womenshealthmag.com/health/g26787041/best-period-tracking-apps/.

3. "Definition of Data Broker - Gartner Information Technology Glossary." Gartner, https://www.gartner.com/en/information-technology/glossary/data-broker.

4. Clue. "We hear your questions & we understand your concerns. The thought that US authorities could use people's private health data against them is infuriating & terrifying. Without fuelling further fear or speculation, we do want to offer our community clarity & reassurance. #RoevWade `." Twitter, Twitter, 25 June 2022, https://twitter.com/clue/status/1540778272727990273.

5. Cole, Samantha. "The #1 Period Tracker on the App Store Will Hand Over Data Without a Warrant [UPDATED]." Vice, 27 June 2022, https://www.vice.com/en/article/y3pgvg/the-1-period-tracker-on-the-app-store-will-hand-over-data-without-a-warrant.

6. "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers about the Disclosure of Their Health Data." Federal Trade Commission, 28 Jan. 2021, https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

7. "Flo Health, Inc.." Federal Trade Commission, 1 Dec. 2021, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

8. Schechner, Sam, and Mark Secada. "You Give Apps Sensitive Personal Information. Then They Tell Facebook." The Wall Street Journal, Dow Jones & Company, 25 June 2022, https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

9. Wetsman, Nicole, and Corin Faife. "Flo Period Tracker Launches 'Anonymous Mode' to Fight Abortion Privacy Concerns." The Verge, The Verge, 14 Sept. 2022, https://www.theverge.com/2022/9/14/23351957/flo-period-tracker-privacy-anonymous-mode.

10. Hunter, Tatum. "Companies Are Hoarding Personal Data about You. Here's How to Get Them to Delete It." The Washington Post, WP Company, 26 Sept. 2021, https://www.washingtonpost.com/technology/2021/09/26/ask-company-delete-personal-data/.

11. Albert, Kendra, et al. "Fear, Uncertainty, and Period Trackers." Medium, Medium, 28 June 2022, https://medium.com/@Kendra_Serra/fear-uncertainty-and-period-trackers-340ab8fdff74.

12. Koebler, Jason, and Anna Merlan. "This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion." VICE, 9 Aug. 2022, https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion.

13. Barrett, Brian. "WhatsApp Fixes Its Biggest Encryption Loophole." Wired, Conde Nast, 10 Sept. 2021, https://www.wired.com/story/whatsapp-end-to-end-encrypted-backups/.

14. Greenberg, Andy. "You Can Finally Encrypt Facebook Messenger, so Do It." Wired, Conde Nast, 4 Oct. 2016, https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/.

15. Eoyang, Mieke, and Michael Garcia. "Weakened Encryption: The Threat to America's National Security – Third Way." Third Way, 9 Sept. 2020, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security.

16. "The Apple-FBI Debate over Encryption." NPR, https://www.npr.org/series/469827708/the-apple-fbi-debate-over-encryption.

17. Crumpler, William, and Jennifer Daskal. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge." Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge | Center for Strategic and International Studies, 25 July 2018, https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.

18. Nakashima, Ellen, and Reed Albergotti. "The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm." The Washington Post, WP Company, 14 Apr. 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.

19. "AB-1242 Reproductive Rights." California Legislative Information, 28 Sept. 2022, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB1242.

20. Curley, Jordan. "Assemblymember Bauer-Kahan and Attorney General Bonta's Legislation Protecting Digital Information on Abortion Heads to the Governor." Official Website - Assemblymember Rebecca Bauer-Kahan Representing the 16th California Assembly District, 31 Aug. 2022, https://a16.asmdc.org/press-releases/20220831-assemblymember-bauer-kahan-and-attorney-general-bontas-legislation.

21. Locke, Phil. "Cell Tower Triangulation – How It Works." Wrongful Convictions Blog, 1 June 2012, https://wrongfulconvictionsblog.org/2012/06/01/cell-tower-triangulation-how-it-works/.

22. Freed, Benjamin. "California Lawmakers Approve Bill Creating 'Data Haven' for Abortion." StateScoop, 1 Sept. 2022, https://statescoop.com/california-abortion-data-privacy-haven/.

23. Kaste, Martin. "Nebraska Cops Used Facebook Messages to Investigate an Alleged Illegal Abortion." NPR, NPR, 12 Aug. 2022, https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion.

24. Cox, Joseph. "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics." VICE, 3 May 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

25. "Dox Definition & Meaning." Merriam-Webster, Merriam-Webster, https://www.merriam-webster.com/dictionary/dox.

26. Raymond, Nate. "Firm Settles Massachusetts Probe over Anti-Abortion Ads Sent to Phones." Reuters, Thomson Reuters, 4 Apr. 2017, https://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX.

27. "Warren Announces Two Key Data Brokers' Commitment to Permanently Stop Selling Location Data of People Seeking Abortion Services." Elizabeth Warren Senate Office, 7 July 2022, https://www.warren.senate.gov/newsroom/press-releases/warren-announces-two-key-data-brokers-commitment-to-permanently-stop-selling-location-data-of-people-seeking-abortion-services.

28. Valentino-DeVries, Jennifer, et al. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." The New York Times, The New York Times, 10 Dec. 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

29. Cox, Joseph. "The Inevitable Weaponization of App Data Is Here." VICE, 21 July 2021, https://www.vice.com/en/article/pkbxp8/grindr-location-data-priest-weaponization-app.

30. Ng, Alfred. "'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions." POLITICO, 18 July 2022, https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906.

31. Fussell, Sidney. "An Explosion in Geofence Warrants Threatens Privacy across the US." Wired, Conde Nast, 27 Aug. 2021, https://www.wired.com/story/geofence-warrants-google/.

32. Eastern District of Virginia, Richmond Division. United States of America v. Okello T. Chatrie. 3 Mar. 2022. https://www.documentcloud.org/documents/22081892-lauck-opinion.

33. Fitzpatrick, Jen. "Protecting People's Privacy on Health Topics." Google, Google, 1 July 2022, https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

34. "Warner, Slotkin, Colleagues Urge Action on Misleading Search Results about Abortion Clinics." Mark R. Warner, 17 June 2022, https://www.warner.senate.gov/public/index.cfm/2022/6/warner-slotkin-colleagues-urge-action-on-misleading-search-results-about-abortion-clinics.

35. Feiner, Lauren. "Google Will Only Show Verified Abortion Providers by Default When Users Search for Clinics." CNBC, 25 Aug. 2022, https://www.cnbc.com/2022/08/25/google-to-show-verified-abortion-providers-by-default-in-clinic-search.html.

36. Allyn, Bobby. "Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers." NPR, NPR, 11 July 2022, https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions.

37. Fishing Expedition." Legal Information Institute, Legal Information Institute, https://www.law.cornell.edu/wex/fishing_expedition.

38. Schuppe, Jon. "Police Sweep Google Searches to Find Suspects. the Tactic Is Facing Its First Legal Challenge." NBCNews.com, NBCUniversal News Group, 30 June 2022, https://www.nbcnews.com/news/us-news/police-google-reverse-keyword-searches-rcna35749.

39. Dillon, Raquel Maria. "Google Workers Sign Petition Asking Company to Protect People's Abortion Search Data." NPR, NPR, 18 Aug. 2022, https://www.npr.org/2022/08/18/1118051812/google-workers-petition-abortion-data.

40. Fitzpatrick, Jen. "Protecting People's Privacy on Health Topics." Google, Google, 1 July 2022, https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

41. "Bill 1373." South Carolina Legislature, 28 June 2022, https://www.scstatehouse.gov/sess124_2021-2022/prever/1373_20220628.htm.

42. Collings, Paige. "Victory! South Carolina Will Not Advance Bill That Banned Speaking about Abortions Online." Electronic Frontier Foundation, 26 Aug. 2022, https://www.eff.org/deeplinks/2022/08/victory-south-carolina-will-not-advance-bill-banned-speaking-about-abortions.

43. Vogus, Caitlin. "CDT Joins Letter Opposing South Carolina Senate Bill 1373." Center for Democracy and Technology, 17 Aug. 2022, https://cdt.org/insights/cdt-joins-letter-opposing-south-carolina-senate-bill-1373/.

44. Robertson, Adi. "A South Carolina Plan to Punish Abortion Aid Sites Is Going Nowhere." The Verge, The Verge, 31 Aug. 2022, https://www.theverge.com/2022/8/31/23327122/south-carolina-rejects-nrlc-model-legislation-abortion-law-internet-ban-speech.

45. Bellware, Kim. "South Carolina House Passes Abortion Ban with Rape and Incest Exception." The Washington Post, WP Company, 31 Aug. 2022, https://www.washingtonpost.com/nation/2022/08/31/south-carolina-abortion-bill-debate/.

46. "The Anarchist Cookbook. : With a Prefatory Note on Anarchism Today." Library of Congress Catalog, Library of Congress, https://lccn.loc.gov/71127797.

47. Dokupil, Tony. "Sorry about All the Bombs." Newsweek, 20 Feb. 2011, https://www.newsweek.com/sorry-about-all-bombs-68549.

48. Murphy, Sean. "Clergy, Social Workers Fear Fallout from Okla. Abortion Laws." AP NEWS, Associated Press, 15 Aug. 2022, https://apnews.com/article/abortion-religion-oklahoma-city-c1f66720db215ead0995c8ed7a833354.

49. "Roe v. Wade." Center for Reproductive Rights, https://reproductiverights.org/roe-v-wade/.