Journal of Law and Policy

Volume 31 | Issue 2 Article 8

5-1-2023

Leave Your Phone at Home: Combatting Data Exploitation in a Post-Dobbs America

Danielle Terracciano

LEAVE YOUR PHONE AT HOME: COMBATTING DATA EXPLOITATION IN A POST-*DOBBS* AMERICA

Danielle Terracciano[*]

> [T]he right to be let alone – the most comprehensive of rights, and the right most valued by civilized men.[1]

This Note comments on the dangers of an under-regulated data privacy sphere and highlights the particularly troubling threats posed to individuals seeking reproductive healthcare. In an ever-digitalizing world, smart phone and device users are subjected to violative data practices, like geofencing and location tracking, without their knowledge or consent. Some data service providers use personal data as a commodity to advance advertising or political objectives. Reproductive healthcare patients are at a heightened risk of exploitation because their personal data may infer or reveal their private healthcare decisions. As the fight for bodily autonomy was upended by the Supreme Court's decision in Dobbs v. Jackson Women's Health *in 2022, the lack of data privacy laws pose a heightened risk. One pathway to protection requires enacting a proposed federal law, the ADPPA, to ensure all individuals that their right to be left alone is valued and safeguarded.*

---

[*] Thank you to the Journal of Law & Policy staff for their countless hours of work on bringing this Note to publication. This Note would not have come to fruition without the unwavering support of my parents, Dawn and Anthony. Thank you to my partner, Jonathan, for being a sounding board throughout the writing process and my biggest cheerleader. I would also like to thank my friends, who graciously endured me discussing data brokerage and geofencing for months on end. This Note is dedicated to my late grandmother, Gloria, who intimately understood the fight for women's equality and autonomy.

[1] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

INTRODUCTION

Every day, cell phones collect massive amounts of data about their users, such as their Internet search histories and precise locations.[2] This may seem benign to a user who Google-searches the best banana bread recipe and takes an Uber to the grocery store; however, mass data collection is more troubling when a user researches an abortion provider and takes an Uber to the provider's office. That information exposes the most intimate details of one's life. Without the user's knowledge, data service providers[3] collect, sell, and use non-medical personal data to disrupt healthcare decision-making and to inhibit access to abortion services.[4] This alarming practice led Americans to consider how to avoid data privacy intrusions.[5] In response to fears of location and activity tracking, the United States Department of Health and Human Services ("HHS") preposterously advised future abortion patients to consider "leaving [your phone] at home,"[6] ignoring the reality that many individuals rely on mobile phones to research healthcare providers, book medical services, and travel to appointments.[7] For

---

[2] Jennifer Valentino-Devries et. al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[3] For the purpose of this Note, "data service providers" refers to any entity that collects, sells, or transfers data, such as Internet service providers, mobile applications, data brokers, or other parties.

[4] Valentino-Devries, *supra* note 2; Flora Garamvolgyi, *Why US Women Are Deleting Their Period Tracking Apps*, THE GUARDIAN (June 28, 2022), https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps.

[5] *See* Garamvolgyi, *supra* note 4.

[6] *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 29, 2022), hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

[7] In 2011, the Pew Research Center found that eighty percent of adult internet users have researched health conditions or treatments online. Susannah Fox, *The Social Life of Health Information, 2011*, PEW RSCH. CTR. (May 12, 2011), https://www.pewresearch.org/internet/2011/05/12/the-social-life-of-health-information-2011/;

those individuals, leaving their cell phones at home is unrealistic at best. Even the Supreme Court has recognized that cell phones and their services "are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[8]

Although Americans rely heavily on cell phones, most are worried about mass data collection, sale, and misuse.[9] The dangers of such data abuses are particularly troubling when they arise in the reproductive healthcare context. For instance, advertising executive John Flynn worked on behalf of anti-choice activist groups to exploit abortion patients' personal data and disrupt their medical decisions.[10] In 2015, Flynn began using geofencing technology[11] to identify "abortion-minded women" near or inside reproductive

---

Survey Reveals Patients Want Online Appointment Booking, PATIENTPOP (Nov. 22, 2016), https://www.patientpop.com/blog/online-scheduling-statistics-healthcare/#:~:text=64%20percent%20of%20patients%20will,of%20online%20scheduling%3A%20%243.2%20billion.

[8] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[9] Brooke Auxier et. al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (finding that seventy-nine percent of Americans are concerned about how private companies use their personal data).

[10] One anti-choice group paid Flynn $8,000 for a geofencing campaign. Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, REWIRE NEWS GRP. (May 25, 2016), https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

[11] Geofencing technology creates geographic boundaries around a location through the use of the Global Positioning System (GPS), Internet Protocol (IP) address, Wi-Fi information, and/or Bluetooth technology. When mobile devices enter the perimeter of the geofence, they can be "tagged" or marked, for entities to track. Assurance of Discontinuance at 2–3, *In re* Commonwealth v. Copley Advert., LLC, *Assurance of Discontinuance*, at 2 (2017), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2452&context=historical [hereinafter Copley].

healthcare clinics.[12] When a patient entered the clinic's perimeter,[13] Flynn would "tag" her[14] device as being inside the geofence.[15] Then, if a patient opened a mobile application[16] on her phone, his software would make third-party banner advertisements[17] appear, advising her, "You Have Choices" and "You're Not Alone."[18] If a patient clicked on the advertisements, her device would open an anti-choice website featuring "pregnancy support specialists" who counsel against abortion.[19] Flynn did not stop there; once the patients left the clinic perimeter, he continued to send the advertisements for up to thirty days later.[20] Altogether, he sent anti-choice advertisements to over 800,000 patients across the country.[21] This type of gross data abuse and inability to hold violators like Flynn accountable are some

---

[12] Coutts, *supra* note 10.

[13] The perimeter means "the outermost physical boundary of a Medical Center, including the boundary of any parking garage or parking lot for patrons of the Medical Center that is physically contiguous with the Medical Center." Copley, *supra* note 11, at 6.

[14] For the purposes of this Note, I will use she/her pronouns to refer to abortion patients. However, the use of gendered language is not meant to discount individuals who can become pregnant and do not identify as women.

[15] Coutts, *supra* note 10.

[16] "A mobile application is information accessed through the use of software designed to run on smartphones." Latena Hazard, *Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U.J.L. & TECH. 447, 453 (2017).

[17] Banner advertisements are "the creative rectangular ad[s] that are shown along the top, side, or bottom of a website in hopes that it will drive traffic to the advertiser's proprietary site." *What is Banner Advertising*, AMAZON ADS, https://advertising.amazon.com/library/guides/banner-advertising (last visited Mar. 13, 2023).

[18] Copley, *supra* note 11, at 3.

[19] *Id*. at 3–4.

[20] *Id*. at 4.

[21] Flynn reached 800,000 patients between the ages of eighteen to twenty-four years old during one of his advertising campaigns. Thus, those 800,000 patients entered the vicinity of a Planned Parenthood clinic. Flynn geofenced Planned Parenthood clinics in: New York City; Columbus, Ohio; Richmond, Virginia; St. Louis, Missouri; and Pittsburgh, Pennsylvania. More than 2,000 of those patients tagged actually clicked on the targeted ads Flynn sent, leading them to anti-choice group websites. Coutts, *supra* note 10.

regrettable consequences of an underregulated data privacy sphere.[22]

Unfortunately for individuals like those targeted by Flynn, the legal landscape governing data privacy is fractured, leaving them without recourse.[23] No comprehensive federal data privacy law exists in the United States, and only five state laws govern this issue.[24] As such, data privacy laws are underdeveloped and data practices are abused.[25] The recent Supreme Court decision in *Dobbs v. Jackson Women's Health*,[26] which overturned the constitutional right to access abortion, has brought attention and immediacy to this already critical data privacy crisis by amplifying the stakes. Post-*Dobbs*, reproductive healthcare patients are at risk of surveillance, harassment, and potential criminal charges if their data is exploited.[27] This issue is exacerbated by the fact that mobile devices—and the data they collect—permeate[28] society; even the

---

[22] Notably, Flynn was not held accountable under a data privacy law. Massachusetts' Attorney General, Maura Healey, sued Flynn under state consumer protection law, claiming he participated in unfair and deceptive dealing. Copley, *supra* note 11, at 4–5.

[23] Flynn's case resulted in an order prohibiting him from geofencing abortion clinics in the future. However, the 800,000 people whose data he wrongfully collected received no remedy or damages. *Id*. at 7.

[24] Madeline M. Cook, *Bringing Down Big Data: A Call for Federal Data Privacy Legislation*, 74 OKLA. L. REV. 733, 768, 781(2022).

[25] *See id*.

[26] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2234 (2022).

[27] *See generally* Scott Henson, *Abortion is (Again) a Criminal-Justice Issue*, TEX. OBSERVER (July 13, 2022), https://www.texasobserver.org/abortion-is-once-again-a-criminal-justice-issue/ (arguing that anti-abortion states will revive criminal abortion statutes post-*Dobbs*); Caroline Cuellar, *A Texas Woman Has Been Charged With Murder After a So-Called 'Self-Induced Abortion'*, NPR (Apr. 10, 2022), https://www.npr.org/2022/04/10/1091927639/a-texas-woman-has-been-charged-with-murder-after-a-so-called-self-induced-aborti (reporting that a woman was arrested for self-administering an abortion after a restrictive abortion ban was enacted in Texas); Shalia Dewan & Sheera Frenkel, *A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska*, N.Y. TIMES (Aug. 18, 2022), https://www.nytimes.com/2022/08/18/us/abortion-prosecution-nebraska.html (claiming that the criminal abortion landscape will unravel post-*Dobbs*).

[28] A survey conducted by the Pew Research Center from January 25 to February 8, 2021 found that forty-four percent of eighteen to forty-nine-year-olds

Supreme Court has recognized this since 1979. Indeed, forty-four years ago, Justice Marshall observed that "unless a person is prepared to forgo use of [telephones], what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[29] This sentiment is at odds with HHS's guidance to leave *mobile* phones at *home*, which is entirely impractical and unreasonable in 2023.[30] Therefore, cell phone users are forced to accept the risk of data privacy violations.

This Note examines how an underregulated data privacy sphere leaves people's non-medical data vulnerable to exploitation by anti-choice parties in a post-*Dobbs* America. Part I explains the mechanics of data transactions and introduces how personal data is treated as a commodity. Part II outlines the current legal landscape of data privacy in the United States and compares the existing state and federal pathways to privacy protection. Part III discusses the practical consequences of insufficient privacy laws by sharing stories of data exploitation that threatened personal autonomy and access to abortion care. Part IV assesses *Dobbs*' destructive impact on abortion rights and its powerful threat to personal data privacy. Finally, Part V argues that Congress must pass a comprehensive data privacy statute with a focus on protecting non-medical data from being exploited in medical decision-making circumstances.

I. DATA PRIVACY BASICS

It is a common experience in 2022 to search for a product online and then receive countless advertisements for that type of product shortly thereafter.[31] Before seeing those advertisements, however, software in the device used for the search collects data about the

---

are online almost constantly on smartphone or internet-connected devices. *See* Andrew Perrin and Sara Atske, *About Three-in-Ten U.S. Adults Say They are 'Almost Constantly' Online*, PEW RSCH. CTR. (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/.

[29] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[30] *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, *supra* note 6.

[31] Cook, *supra* note 24, at 734.

user.[32] The software's service provider then sells or transfers the data to a third party.[33] A foundational knowledge of data privacy is essential to understand this type of transaction. Data privacy is the right to dictate how, if at all, one's personal information[34] is collected and used.[35] Personal information may include, among other things, one's name, gender, age, race, precise location, and internet search history.[36] All of this information can be collected and sold without the user's knowledge.[37]

a. Collecting Data

Entities obtain different types of data in different ways.[38] For instance, geolocation information, which provides the precise past or present location of a mobile device,[39] is harvested differently than one's shopping history.[40] Naturally, geolocation data also reveals the location of the individual using the device. It can be obtained through mobile applications ("apps" or "mobile apps") by enabling location services.[41] This may seem innocuous if one enables location services only to check the weekend weather report or traffic delays when commuting home from work. However, a 2018 New York Times investigation into geolocation collection identified serious privacy implications; the dataset it reviewed showed "over 235 million locations captured from more than 1.2 million unique

---

[32] *Id*. at 735.

[33] *Id*.

[34] Personal information is that which identifies a particular person. *Glossary of Privacy Terms*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/glossary/ (last visited Mar. 13, 2023).

[35] *About the IAPP*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/about/what-is-privacy/ (last visited Mar. 13, 2023).

[36] *Glossary of Privacy Terms*, *supra* note 34.

[37] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY at i (2014).

[38] *Id*. at 17.

[39] *Glossary of Privacy Terms*, *supra* note 34.

[40] DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 37, at 17.

[41] Valentino-Devries et al., *supra* note 2.

devices during a three-day period in 2017."[42] One user whose data was collected in the investigation was deeply troubled to learn the extent to which her cell phone tracked her location.[43] She commented that "[i]t's the thought of people finding out those intimate details that you don't want people to know," like visiting a Planned Parenthood clinic, in another user's case.[44]

In other instances, apps collected geolocation data on any given user more than fourteen thousand times per day.[45] Another individual whose data was tracked in the study commented, "[i]t's very scary . . . [i]t feels like someone is following me, personally."[46] As long as the location services setting is enabled, mobile apps can even collect geolocation data when the app itself is not in use, meaning apps can constantly collect data in the background of a device without user knowledge.[47] Notably, mobile apps are just one prominent source of geolocation data; cell phones can also collect a user's geolocation through cell towers, Bluetooth, Wi-Fi, and GPS navigation.[48] Thus, even if a user deletes every app on her device and disables location services, her phone will still collect geolocation data.

Data service providers also regularly collect personal data unrelated to a user's location.[49] Consumer businesses and tech giants use a variety of tactics to obtain personal data like a user's name, demographic information, and internet search history.[50] Providers

---

[42] *Id*.

[43] The Times reviewed anonymized data, but was able to re-identify the users in the dataset because the data was so precise. *Id*.

[44] *Id*.

[45] *Id*.

[46] *Id*.

[47] Samantha V. Ettari, *Using Geolocation Data in Litigation*, PERKINS COIE: E-DISCOVERY BULL. (Dec. 2020/Jan. 2021), https://www.perkinscoie.com/images/content/2/4/244639/LIT-Dec20Jan21-EDiscoveryBulletin-2021Update.pdf.

[48] Copley, *supra* note 11, at 2.

[49] DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 37, at 2.

[50] *Id*.

might ask consumers to submit personal information themselves.[51] For example, when creating a Facebook profile, a user must input her name, gender, birthday, and either her phone number or email address.[52] Asking consumers for their personal information directly is an easy way to collect data, but this only works for consumer-facing businesses.

In addition to collecting data from consumers directly, service providers often use web cookie technology to obtain data.[53] Web cookies are data files that are stored on a device and enable websites to remember information for a later date.[54] First-party cookies are embedded into a website by the site's developers themselves, whereas third-party cookies are placed by other parties, like advertisers.[55] First- and third-party cookies have different effects on consumers. Consider a user who takes the following steps on her cell phone internet browser: first the user searches, "where to buy a pregnancy test;" second, the user clicks on the Duane Reade pharmacy website; third, the user inputs her zip code on Duane Reade's website; finally, the user browses the Duane Reade website to see if her local store has pregnancy tests in stock. The next time the user searches if any item is in stock at Duane Reade, her internet browser will remember her zip code and automatically show the stock for her local store. This is the result of first-party cookies

---

[51] Gabe Turner & Aliza Vigderman, *The Data Big Tech Companies Have On You*, SECURITY.ORG (Oct. 10, 2022), https://www.security.org/resources/data-tech-companies-have/.

[52] FACEBOOK, https://www.facebook.com/reg/ (last visited Mar. 13, 2023); *see, e.g.*, TWITTER, https://twitter.com/i/ flow/signup (last visited Mar. 13, 2023) (collecting the user's name, phone number or email address, and birthday); MACY'S, https://www.macys.com/account/createaccount (last visited Mar. 13, 2023) (collecting the user's name, email address, and birth month and day); HOME DEPOT, https://www.homedepot.com/auth/view/createaccount/diy (last visited Mar. 13, 2023) (collecting the user's email address, zip code, and phone number).

[53] William Goddard, *How Do Big Companies Collect Customer Data?*, IT CHRON. (Jan. 14, 2019), https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data/.

[54] *Glossary of Privacy Terms*, *supra* note 34; Emily Stewart, *Why Every Websites Wants You to Accept Its Cookies*, VOX (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy.

[55] Stewart, *supra* note 54.

placed by the pharmacy's website itself.[56] Alternatively, when the user is browsing on a different website, perhaps one for holiday shopping, she may still see banner advertisements for pregnancy tests. This is a result of third-party cookies, which tracked the user's searches and analyzed her data to present her with a targeted advertisement.[57]

Rather than collecting data itself, a company can buy data from data brokers,[58] which are companies that collect, aggregate, analyze, and sell consumer information "for purposes such as marketing products, verifying an individual's identity, or detecting fraud."[59] Unlike retail businesses, data brokers do not interact with consumers directly.[60] For this reason, they turn to web crawling,[61] a data collection method whereby software combs through the Internet for relevant data and remits it back to the broker's servers. [62] The software identifies "which websites to crawl, how often, and what data points to collect from each website."[63]

b. Buying and Selling Data

Buying and selling data is not a practice exclusive to data brokers. Indeed, selling or shopping for data is accessible to the regular internet user.[64] Any individual can visit an online data marketplace, like databroker.global ("the Platform"), a "one-stop solution for buying and selling data,"[65] to buy or sell data from the

---

[56] *See id*.

[57] Targeted advertising is a marketing tactic that tailors advertisements to a consumer's interests, based on patterns found in her data. *See generally* DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 37, at i.

[58] *Id*.

[59] *Id*. at 3.

[60] *Id*. at 46.

[61] *Id*. at 17.

[62] *Id*.

[63] Web crawling is one method data brokers use to collect data without consumers' knowledge. *Id*.

[64] *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[65] DATABROKER, https://test.databroker.global/ (last visited Mar. 13, 2023).

comfort of her own home. By visiting the Platform's website, interested individuals can browse some of the datasets available for purchase, filtering the search options to the "people" and "health" categories to see that the following data sets are available for purchase: "[d]ata contained various information like Name, Email, Contact, SSN"[66] and "I have 30MM USA consumer data -500K CBD, 5MM ME, 25 MM (knee, joint pain, diabetes, health)."[67] Some of the data on the Platform is free to download, while other datasets must be purchased.[68] The Platform operates just like many retailers do—they accept payment by debit or credit cards, allow you to view your purchase history, and even offer a thirty-day warranty on your purchase.[69]

Buying data is unsettlingly easy and inexpensive.[70] In May 2022, a Vice reporter bought one week's worth of location data on more than 600 Planned Parenthood clinics for approximately $160.[71] Vice bought the dataset from SafeGraph, a data broker that "obtains location data from ordinary apps installed on peoples' phones."[72] Not all of the Planned Parenthood locations in that dataset provided abortion services, but Vice was able to verify which locations did.[73] Some of the aggregated data that Vice purchased reflected less than five devices having visited a single

---

[66] DATABROKER, https://www.databroker.global/data_marketplace (last visited Mar. 13, 2023); Unlike the dataset being sold here, typically, when data is bought or sold, it does not directly identify the person it belongs do. The data is often linked to "a string of numbers called an "identifier"" that corresponds to the dataset. Tatum Hunter & Jeremy Merrill, *Health Apps Share Your Concerns with Advertisers. HIPAA Can't Stop It.*, WASH. POST (Sept. 22, 2022), https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/.

[67] DATABROKER, *supra* note 66.

[68] *See generally* DATABROKER, *supra* note 65.

[69] *Beginner's Guide to Buying Data*, DATABROKER, https://www.databroker.global/help/buying-data/topic/beginner%E2%80%99s-guide-to-buying-data (last visited Mar. 13, 2023).

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

[71] *Id*.

[72] *Id*.

[73] *Id*.

Planned Parenthood location.[74] SafeGraph's dataset did not provide the device owners' names, but Vice claimed that it is possible to deanonymize the data because parts of the dataset tracked so few devices.[75]

II. DATA PRIVACY LEGAL LANDSCAPE

As one cybersecurity professional commented, selling abortion clinic location data is "bonkers dangerous" and may lead to serious privacy intrusions.[76] However, because the United States does not have a comprehensive[77] federal data privacy law, there is no overarching legal authority prohibiting this type of data transaction.[78] Instead, data privacy governance is fragmented. Two federal statutes and five state laws are noteworthy when considering the intersection between data privacy and abortion healthcare.[79]

a. Federal Laws

When considering data violation risks in a post-*Dobbs* America, two federal laws—the Health Insurance Portability and Accountability Act ("HIPAA") and the Federal Trade Commission

---

[74] *Id*.

[75] SafeGraph aggregates its data by tracking the location of groups of devices, rather than a singular device. When a service provider aggregates data, it categorizes consumers by identifying factors and bundles their data with that of similar consumers. This allows the service provider to make inferences about a certain "type" of consumer. *Id*.

[76] *Id*.

[77] A comprehensive privacy law is one like Europe's General Data Protection Regulation ("GDPR"), which governs data practices in all sectors. Compare the Health Insurance Portability and Accountability Act ("HIPAA"), the Fair Credit Reporting Act ("FCRA"), and the Family Educational Rights and Privacy Act ("FERPA"). Each of these federal privacy laws govern distinct sectors. HIPAA keeps private information between patients and health providers, the FCRA protects personal credit report data, and FERPA governs student education records privacy. This differs from Europe's GDPR, which applies to privacy in the healthcare, personal finance, education, and all other sectors. Klosowski, *supra* note 64.

[78] Cook, *supra* note 24, at 768.

[79] *Id.*

Act ("FTC Act") stand out. Unlike the FTC Act, which regulates all industries, HIPAA is healthcare sector-focused.[80] HIPAA requires that personal health information be kept confidential between patients and healthcare providers unless a patient consents to disclosure.[81] Thus, HIPAA is not particularly useful when seeking to protect non-medical personal data from exploitation by anti-choice parties. Medical information is protected under HIPAA, but non-medical personal data is not.[82]

The current issue is not that anti-choice parties are obtaining individual's medical records; rather, the datasets at risk are Internet search histories, purchase patterns, geolocation data, and other personal data.[83] When this data is viewed together, anti-choice parties can infer an individual's reproductive healthcare choices or intentions.[84] Latena Hazard argued that HIPAA should be expanded to govern entities like health-related mobile applications, which are not yet covered by the statute.[85] Currently, HIPAA does not govern user privacy on menstruation or fertility tracking apps because the relevant health information is provided by a user, rather than a medical doctor or provider.[86] In addition to widening HIPAA's scope, Hazard argued that the FTC must enforce health privacy regulations to meaningfully protect patients and consumers.[87]

Proponents of expanding HIPAA may find comfort in the FTC Act's broad scope.[88] The FTC Act outlaws "unfair or deceptive acts

---

[80] *See* 45 C.F.R. § 164.104.

[81] 45 C.F.R. § 164.502.

[82] *See* 45 C.F.R. § 160.103.

[83] *Explainer: Online Privacy in a Post-Roe World*, THE ASSOCIATED PRESS (Aug. 10, 2022), https://apnews.com/article/abortion-us-supreme-court-technology-health-c62b071aae11783fe0aeed99bbf8fffc.

[84] *See id*.

[85] *See* Hazard, *supra* note 16, at 465.

[86] Jeannie Baumann, *Fertility Apps Bound by Weak Disclosure Rules in Post-Roe World*, BLOOMBERG LAW (May 18, 2022), https://news.bloomberglaw.com/pharma-and-life-sciences/fertility-apps-bound-by-weak-disclosure-rules-in-post-roe-world; 45 C.F.R. § 160.103.

[87] Hazard, *supra* note 16, at 473.

[88] *See* F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972) (explaining that the FTC Act applies across many industries because it is impossible for Congress to identify all instances in which unfair practice might occur).

or practices in or affecting commerce,"[89] which is flexible and designed to account for "evolving content."[90] When drafting the FTC Act, Congress "explicitly considered, and rejected" identifying sectors in which unfair business practices occur, so the Federal Trade Commission's ("FTC") authority applies across all industries.[91] When challenging unfair and deceptive practices, the FTC can bring enforcement actions[92] in civil court or can initiate administrative adjudication actions before the Commission.[93]

The FTC might bring an enforcement action when a business engages in an unfair practice—one that "is likely to cause substantial injury to customers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[94] Similarly, the FTC can bring an enforcement action for deceptive practices by establishing, "first, [that] there is a representation, omission, or practice that, second, is likely to mislead consumers acting reasonably under the circumstances, and third, the representation, omission, or practice is material."[95]

---

[89] 15 U.S.C. § 45(a)(1).

[90] F.T.C. v. Bunte Bros., 312 U.S. 349, 353 (1941).

[91] F.T.C. v. Sperry & Hutchinson Co., 405 U.S. at 239–40 (holding that the FTC can pursue unfair commercial practice actions beyond those with antitrust consequences); *see* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 501 (2020).

[92] 15 U.S.C. § 45(m).

[93] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, THE FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority. The FTC can also issue "soft law" in the form of investigative reports, recommendations to Congress, or best practice guidelines which identify unfair or deceptive business practices and advise how entities can avoid engaging in them. Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 COMPETITION: J. ANTI., UCL & PRIVACY SEC. ST. B. CAL. 89, 91 (2016); Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 792 (2016).

[94] 15 U.S.C. § 45(n).

[95] Matter of Cliffdale Associates, Inc., 103 F.T.C. 110 (1984).

Due to its broad authority, the FTC Act has been used as a catchall law for rectifying data privacy intrusions.[96] Because data privacy practices fall under the FTC's purview, the Commission brought actions against data service providers for unfair and deceptive practices for over twenty years.[97] In 1999, the Commission brought its first enforcement action against a data broker, Touch Tone Information, Inc. ("Touch Tone"), in a federal district court claiming that it obtained consumers' private financial information without their knowledge and sold it to other entities.[98] Touch Tone allegedly obtained this information by calling financial institutions and impersonating account holders, which the FTC argued was a material misrepresentation that was likely to mislead consumers in violation of the statute.[99] The consumer-friendly district court took a major step towards protecting data privacy by ordering Touch Tone to provide consumers with a privacy notice when collecting personally identifying information, effectively limiting data brokers' ability to transact without consumer knowledge.[100]

Following its case against Touch Tone, the FTC continued to be an enforcer of data privacy protections.[101] Recently, the

---

[96] The FTC's overarching mission is "protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education." *Mission*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission (last visited Feb. 20, 2023); *see also* Hazard, *supra* note 16, at 463.

[97] Reicher & Fang, *supra* note 93, at 93.

[98] F.T.C. v. Rapp, No. 99-WM-783, 2000 U.S. Dist. LEXIS 20627 at *1–2 (D. Colo. 2000).

[99] *Id*.

[100] *Id*. at *8–9. The district court also enjoined Touch Tone from making any further misleading statements to obtain consumer financial information. *Id*. at *4–5.

[101] *See, e.g.*, F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1191 (10th Cir. 2009) (affirming the District Court's award of injunctive relief against a website for selling consumer telephone records); Final Judgment and Order, F.T.C. v. Sitesearch Corp., No. CV-14-02750 (PHX) (NVW) (D. Ariz. Feb. 18, 2016) (enjoining a data broker from selling or disclosing consumer financial and sensitive data); Final Judgment and Order, F.T.C. v. EchoMetrix, Inc., No. 2:10-CV-05516 (DRH) (ARL) (E.D.N.Y. Nov. 30, 2010) (ordering a software developer to destroy improperly retained and stored consumer data).

Commission took a marked interest in pursuing entities that violate reproductive healthcare privacy. In 2021, the FTC initiated an administrative action against FloHealth, Inc., a fertility and menstruation tracking app used by over one hundred million consumers.[102] The Commission's Bureau of Consumer Protection claimed that FloHealth disclosed millions of users' personal data, including the user's intention to get pregnant and her menstrual cycle dates, to third parties for marketing and analytics purposes despite promising to keep user data confidential.[103] After the Commission's administrative review concluded that FloHealth's practices were unfair and deceptive, the parties reached a settlement.[104] To protect consumer data privacy, the FTC's settlement ordered FloHealth to stop misrepresenting its privacy practices and to begin notifying consumers of what information it discloses to third parties.[105] The FloHealth case exemplifies how the FTC has stepped in to protect data privacy rights when consumers are not otherwise protected by federal laws, like HIPAA.

b. State Laws

As a supplement to the FTC's efforts, five states—California,[106] Connecticut,[107] Colorado,[108] Virginia,[109] and Utah[110]—enacted comprehensive data privacy laws to protect consumers in their respective states. Each of the five state laws impose unique

---

[102] *FTC Finalizes Order with Flo Health*, THE FED. TRADE COMM'N (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.

[103] Complaint, In the Matter of Flo Health, Inc., Docket No. C-4747, F.T.C. (2021); *see also* Alisha Haridasani Gupta & Natasha Singer, *Your App Knows You Got Your Period. Guess Who it Told?* N.Y. TIMES (Jan. 28, 2021), https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html.

[104] *FTC Finalizes Order with Flo Health*, *supra* note 102.

[105] *Id.*

[106] CAL. CIV. CODE §798.105 (2011).

[107] 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §3.

[108] COLO. REV. STAT. §6-1-1301.

[109] VA. CODE ANN. §59.1-578.

[110] UTAH CODE ANN. §13-61-403.

obligations on business entities and afford individuals a range of privacy protections, but they are not homogeneous.[111] Their lack of uniformity created a patchwork legal scheme, making compliance with each statute challenging for covered entities.[112]

In 2018, California pioneered the first comprehensive state privacy law, the California Consumer Privacy Act ("CCPA"), the gold standard of state privacy laws due to its many protections.[113] The CCPA affords consumers the right to know what data an entity has collected and the power to request that the entity delete their data.[114] The CCPA also grants individuals a global opt-out right which allows consumers to opt-out of companies selling or sharing their data from a single browser, rather than having to do so within each individual website.[115] Most critically, the CCPA grants citizens a private right of action, allowing consumers to sue data service providers who violate their rights protected under this statute.[116] Additionally, the CCPA imposes obligations on entities doing business in California.[117] These obligations only apply to for-profit businesses and do not regulate government entities or non-profit organizations.[118] For-profit businesses must provide consumers with notice of the types of personal information they collect, the types of third parties with whom they share data, the purpose for which they collect and share data, and from where they sourced the data.[119]

In 2020, California amended the CCPA with the California Privacy Rights Act ("CPRA"), which, among other things, grants

---

[111] Cook, *supra* note 24, at 781.

[112] *Id.*

[113] *Id.* at 776; *see also* Klosowski, *supra* note 64.

[114] CAL. CIV. CODE §1798.105.

[115] Klosowski, *supra* note 64.

[116] CAL. CIV. CODE §1798.150.

[117] *Id*. at §§1798.110–20.

[118] The CCPA governs private entities that (1) generate annual gross revenues of twenty-five million dollars or more, (2) collect, buy, sell, or share fifty thousand dollars or more consumers personal information annually, or (3) sell enough consumer personal data to account for at least fifty percent of annual revenues. CAL. CIV. CODE § 1798.140.

[119] *Id*. at §§ 1798.110–20; *California Privacy Rights Act: An Overview*, PRIVACYRIGHTS.ORG (Dec. 10, 2020), https://privacyrights.org/resources/california-privacy- rights-act-overview.

individuals the right to correct any inaccurate information collected by data service providers.[120] The amendment also imposes a data minimization obligation, forbidding businesses from retaining personal data for longer than necessary to achieve the purpose for which it was collected.[121] Finally, the CPRA requires a business to notify consumers when it collects, uses, sells, or shares "sensitive personal information,"[122] including a consumer's precise geolocation; this is particularly relevant to the ongoing challenge of protecting patient's privacy, since geolocation data can infer whether an individual has sought abortion care.[123]

California's "groundbreaking"[124] and historic privacy statute prompted other states to pass comprehensive privacy laws;[125] Connecticut,[126] Colorado,[127] Virginia,[128] and Utah[129] successfully passed data privacy statutes that become effective in 2023.[130] These four state laws, like California's, grant consumers the rights to have businesses delete their personal data, opt-out of data sales, know what personal information a company has collected, and receive notice when their data is collected.[131] However, the Connecticut, Colorado, Virginia, and Utah laws are less protective and less effective than the CCPA and CPRA. One critic argued that Virginia's law is "business-model affirming" by permitting large companies to continue their existing mass data collection

---

[120] *Id*. at § 1798.106.

[121] *Id*. at § 1798.100.

[122] *Id*.

[123] *Id*. at § 1798.140(o)(1)(G).

[124] Navdeep K. Singh, *What You Need to Know About the CCPA and the European Union's GDPR*, A.B.A. (Feb. 26, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr/.

[125] Cook, *supra* note 24, at 776.

[126] 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §3.

[127] COLO. REV. STAT. §6-1-1301.

[128] VA. CODE ANN. §59.1-578.

[129] UTAH CODE ANN. §13-61-403.

[130] Cook, *supra* note 24, at 781.

[131] COLO. REV. STAT. §6-1-1301; 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §3; UTAH CODE ANN. §13-61-403; VA. CODE ANN. §59.1-578.

practices.[132] Additionally, the Connecticut, Colorado, Virginia, and Utah laws do not issue private rights of action and enforcement is left to the states' attorneys general.[133] Attorneys general might not pursue data privacy violations if that does not comport with their personal beliefs, which is possible given their broad discretion over what cases to pursue.[134] Thus, a private right of action is critical to ensuring that the protections granted to consumers and obligations imposed on businesses are enforced.

III. PRACTICAL CONSEQUENCES OF UNDER-REGULATION

Without sufficient data privacy laws to regulate non-medical data collection, use, and sale, individuals face dangerous consequences like surveillance and harassment.[135] Non-medical data obtained without user knowledge can reveal the most private and deeply personal details of one's life. First, Internet search history data could detail a user's research on pregnancy symptoms, abortion procedures, and abortion provider information.[136] Second, purchase pattern data could divulge a consumer's past orders for

---

[132] Klosowski, *supra* note 64.

[133] *Id*.

[134] Attorneys general, like all prosecutors, have discretion over what legal matters to pursue. This could be problematic in states with anti-choice attorneys general in control. In those states, prosecutors might not be sympathetic to data privacy abuse victims when the context the violation arises in is abortion. *See* Bruce A. Green, *Prosecutorial Discretion: The Difficulty and Necessity of Public Inquiry*, 123 DICK. L. REV. 589, 611–612 (2019).

[135] Margi Murphy, *Anti-Abortion Centers Find Pregnant Teens Online, Then Save Their Data*, BLOOMBERG (June 27, 2022), https://www.bloomberg.com/news/articles/2022-06-27/anti-abortion-centers-find-pregnant-teens-online-then-save-their-data.

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

emergency contraception[137] or pregnancy tests.[138] Third, menstruation or fertility tracking apps could indicate pregnancy status.[139] Finally, geolocation data could confirm a patient's visit to an abortion clinic.[140] The United States Supreme Court has even recognized that location tracking "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[141] These types of sensitive data are unknowingly collected and used by businesses and anti-choice parties, making privacy intrusions collateral damage.[142]

a. The Predators: Businesses and Anti-Choice Activists

Anyone with an interest in using other people's sensitive data for a personal or political agenda can do so, thus becoming a predator for data privacy.[143] John Flynn[144] is a predator who exploited personal data for financial gain,[145] whereas Wisconsin's 2022 Republican Gubernatorial candidate, Tim Michels, allegedly engaged in similar data practices in alignment with his political

---

[137] Emergency contraception, commonly known as the "Morning-After Pill" is an over-the-counter contraceptive used after sex to stop a pregnancy before it starts. *Emergency Contraception*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/learn/morning-after-pill-emergency-contraception (last visited Mar. 13, 2023).

[138] Purchase pattern data is sourced by entities themselves, third-party cookies, and web crawlers. This data may reveal the following information about a consumer's purchase: type product or services bought, amount bought, time and location of purchase, payment method, and demographic information about the consumer. *Consumer Purchase Data*, EXPLORIUM, https://www.explorium.ai/wiki/consumer-purchase-data/ (last visited Mar. 13, 2023).

[139] *See* Hazard, *supra* note 16, at 473.

[140] Coutts, *supra* note 10.

[141] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[142] *See* Murphy, *supra* note 135; Ng, *supra* note 136.

[143] *See* Cox, *supra* note 70.

[144] *See* Coutts, *supra* note 10.

[145] *Id*.

beliefs.[146] According to Michel's public tax filings from 2010, 2011, and 2015, he contributed to the Veritas Society,[147] an anti-choice organization that exists to dissuade patients from having abortions.[148] The organization's website touts that it collects geolocation data on reproductive health clinics and then puts an "[anti-abortion] message in the right place at the right time."[149] Veritas even goes beyond using targeted advertisements by "reach[ing] these women on apps, social media feeds and websites like Facebook, Instagram, [and] Snapchat with [anti-abortion] content and messaging."[150]

While Michels and Flynn are merely anti-choice individuals, anti-choice institutions,[151] like Veritas, may be even more dangerous predators to data privacy. For decades, the anti-choice movement has used its "insidious power" to reduce abortion access and dissuade women from choosing the treatment, resorting to coaxing and trickery when necessary.[152] One way anti-choice groups reach

---

[146] Tyler Eddy & Charles Benson, *Truth Be Told: Campaign Ad Accuses Tim Michels of Tracking Women Near Abortion Clinics*, TMJ4 (Oct. 11, 2022), https://www.tmj4.com/decision2022/truth-be-told-campaign-ad-accuses-michels-of-tracking-women-near-abortion-clinics.

[147] VERITAS SOCIETY, https://veritassociety.com/ (last visited Mar. 13, 2023).

[148] Eddy & Benson, *supra* note 146.

[149] VERITAS SOCIETY, *supra* note 147.

[150] *Id*.

[151] Anti-choice institutions, organizations, or groups are coalitions of people who advocate against abortion rights. *The Insidious Power of the Anti-Choice Movement*, NARAL (2018), https://www.prochoiceamerica.org/report/insidious-power-anti-choice-movement/ (last visited Mar. 13, 2023). Other anti-choice institutions include: Center for Family & Human Rights, https://c-fam.org/; Susan B. Anthony Pro-Life America, https://sbaprolife.org/; The Elliot Institute, http://www.theunchoice.com/elliotinstitute.htm; and Operation Save America, https://www.operationsaveamerica.org/.

[152] To accomplish its goals, the anti-choice movement spreads misinformation about abortion procedures, protests in front of reproductive healthcare clinics, and lobbies conservative politicians. *The Insidious Power of the Anti-Choice Movement*, *supra* note 151; *see also* Julie Rikelman & Amy Myrick, *If The Court Can't Force CPCs To Tell The Truth, It Can't Force Abortion Providers To Lie*, HUFFINGTON POST (June 27, 2018), https://www.huffpost.com/e

pregnant individuals is through crisis pregnancy centers ("CPCs"), which are brick and mortar anti-abortion advocacy operations.[153] CPCs masquerade as legitimate reproductive health clinics that offer prenatal health care and testing, but they often do not employ licensed medical professionals.[154] Rather than providing neutral advice grounded in medical science, CPCs spread misinformation about abortion to deprive patients of their autonomy and scare them into carrying the pregnancy to term.[155]

CPCs are a physical iteration of the anti-abortion movement; in an ever-digitalizing world, these groups have made robust efforts to promote their beliefs online.[156] Human Coalition is one anti-choice group that began as a "data-driven online marketing and referral service" for CPCs, but then grew into a large CPC network and advocacy group.[157] Human Coalition "shift[ed] the battle to people's phones and computers, [by relying] on search engine optimization, targeted digital ads and an arsenal of websites that *look like* local health clinics" to find abortion patients.[158] Indeed, anti-choice organizations survive and thrive on data. While CPCs and anti-choice groups are extremely dangerous and influential, they are not the only parties with a stake in non-medical data collection and abuse.

---

ntry/opinion-rikelman-myrick-supreme-court-crisis-pregnancy-abortion_n_5b3398c2e4b0cb56051e0aaa.

[153] Kimiko de Freytas-Tamura, *In New York, Anti-Abortion Centers Outnumber Abortion Clinics*, N.Y. TIMES (June 25, 2022), https://www.nytimes.com/2022/06/25/nyregion/crisis-pregnancy-centers-abortion-nyc.html.

[154] *What are Crisis Pregnancy Centers?*, PLANNED PARENTHOOD, (Nov. 4, 2021), https://www.plannedparenthood.org/blog/what-are-crisis-pregnancy-centers.

[155] "Pregnant women have been told that abortions can cause cancer and sterility, and other claims that are medically unproven." Freytas-Tamura, *supra* note 153.

[156] Emma Cott et al., *They Searched Online for Abortion Clinics. They Found Anti-Abortion Centers.*, N.Y. TIMES (June 23, 2022), https://www.nytimes.com/interactive/2022/us/texas-abortion-human-coalition.html.

[157] *Id*.

[158] *Id*. (emphasis added).

Retail businesses also capitalize on consumer data through predatory practices.[159] Retail giant Target's mass data collection and analysis methods are particularly shocking.[160] Target tasked data professional Andrew Pole with creating an algorithm to determine if customers are pregnant, intending to "figure out how to exploit them."[161] Pole used web crawling software[162] to collect and review consumers' purchase patterns and then generated "pregnancy prediction" scores.[163] This software would collect purchase data on items such as unscented lotion, magnesium supplements, and large diaper-bag style purses, relying on that data to foretell whether a shopper was pregnant, and if so, the estimated delivery date.[164] Target took full advantage of the pregnancy prediction tool by sending the potentially pregnant customer baby-related advertisements and coupons.[165]

Pole's pregnancy predictor might appear harmless or even helpful when it results in coupons for customers, but it had a striking impact on one Minneapolis teenager. Target's pregnancy predictor determined that the high-schooler was likely pregnant, so the store mailed her coupons for baby supplies.[166] The young girl's father found the coupons, barged into his local Target store, and angrily accused a store manager of encouraging his daughter to get pregnant.[167] Shortly after his public outburst, the girl's father

---

[159] DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 37, at 13.

[160] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[161] *Id.*

[162] *See* DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 37.

[163] Duhigg, *supra* note 160.

[164] Unscented lotion, magnesium, and diaper-bag sized purses are some of 25 products Pole identified as being relevant to pregnancy. To estimate one's delivery date, Target's data professionals analyzed "how shopping habits changed as a woman approached her due date," which women using Target's baby shower registry feature had willingly disclosed. Then, the analysts extrapolated that data and applied it to customers who did not use the registry feature. *Id*.

[165] *Id*.

[166] *Id*.

[167] *Id*.

learned that his daughter actually was pregnant; Target knew before he did.[168] This anecdote raises a variety of concerns for the pregnant girl. Perhaps she kept her pregnancy private in fear that her father would not allow her to have an abortion or that she would be forced out of the house due to her pregnancy. Even if the teen did not experience adverse repercussions, the pregnancy predictor at least took away her decision to inform her father of her pregnancy. This is undoubtedly disruptive—Target's data practices intruded into this teen's familial relationships and forced conversations about a deeply personal and sensitive issue.

b. The Prey: Mobile Device Users of Child-Bearing Age

Justice Marshall's 1979 claim that all telephone users are forced to accept the risk of surveillance still rings true over forty years later.[169] Over the past forty-four years, individuals have steadily replaced their landline phones for the now-predominant mobile or smart phone.[170] As long as cell phones remain an integral facet of participating in society and the data privacy legal landscape continues to be underregulated, all smartphone users are at risk of non-medical data privacy violations. While virtually anyone with a smartphone can be subjected to anti-choice propaganda, people of child-bearing age are particularly susceptible to their influence.

People of child-bearing age[171] with the ability to become pregnant are at a heightened risk because anti-choice parties seek to dissuade pregnant people from having abortions. Those people

---

[168] *Id*.

[169] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[170] Mike Vorhaus, *Americans Use Their Mobile Phone to Replace Their Landline Phones*, FORBES (May 14, 2021), https://www.forbes.com/sites/mikevorhaus/2021/05/14/americans-use-their-mobile-phone-to-replace-their-landline-phones/?sh=66430db168cc.

[171] Individuals can become pregnant when they ovulate for the first time. *Can You Get Pregnant at Any Age?* PLANNED PARENTHOOD (Sept. 1, 2010), https://www.plannedparenthood.org/learn/ask-experts/can-you-get-pregnant-at-any-age. However, the World Health Organization defines reproductive age as between 15 and 49 years old. *The Global Health Observatory*, WORLD HEALTH ORG. (last visited Mar. 13, 2023), https://www.who.int/data/gho/indicator-metadata-registry/imr-details/women-of-reproductive-age-(15-49-years)-population-(thousands).

living in states that outlaw abortion only weeks after contraception face a sharpened threat: patients have an unreasonably short timeframe to consider their options and correct any misinformation spread by anti-choice activists.[172] One nineteen-year-old, Lisa, was the ideal prey for anti-abortion advocates at a CPC: she was pregnant, young, and impressionable.[173]

After conducting a Google search on her abortion options, Lisa saw an advertisement for a local pregnancy clinic offering free pregnancy tests, but she was unaware that this "clinic" was actually a CPC and not a legitimate healthcare provider.[174] During her appointment at the CPC, Lisa sat in a consultation room "filled with posters depicting fetuses with speech bubbles, as if they were asking to be born."[175] A consultant advised Lisa that she was pregnant, ordered her *not* to get an abortion, and instructed her to return in four weeks for an ultrasound.[176] During her visit, Lisa became concerned about the clinic's legitimacy and asked the receptionist whether her visit information would be kept private.[177] In response, the receptionist avoided her question and shamed her by saying, "Well, honey, this is what happens when you have sex."[178] It was only after Lisa later obtained an abortion elsewhere when she learned that the CPC entered her personal information into a database without her

---

[172] *See, e.g.*, TEX. HEALTH & SAFETY CODE § 171.205(a) (prohibiting abortions after a fetal heartbeat has been detected, typically around the sixth week of gestation); Georgia, Idaho, Iowa, Kentucky, Louisiana, Mississippi, North Dakota, Ohio, Oklahoma, South Carolina, and Tennessee also ban abortion as early as six weeks of pregnancy. *Bans on Abortion by Week* at 2, NARAL, https://www.prochoiceamerica.org/wp-content/uploads/2022/01/WHODecides2022-BANS-BY-WEEK-Report-011722-1.pdf.

[173] "Lisa" is an alias to protect the teenager's identity. Murphy, *supra* note 135.

[174] *What are Crisis Pregnancy Centers?*, *supra* note 154; Murphy, *supra* note 135.

[175] Murphy, *supra* note 135.

[176] *Id*.

[177] *Id*.

[178] *Id*.

knowledge or approval.[179] The CPC then harassed Lisa for weeks by frequently calling her and asking for updates on her "baby."[180] While this type of harassment is inexcusable, a recent Supreme Court decision amplified the consequences of data privacy violations.

IV. *DOBBS*' DETRIMENTAL IMPACT ON DATA PRIVACY

Fifty years ago, the Supreme Court crystallized the constitutional right to access an abortion in the landmark case *Roe v Wade*. [181] In *Roe*, the Court heard a challenge to a Texas criminal statute that outlawed abortions at any point during a pregnancy, except if necessary to save the pregnant person's life.[182] The Court opined that one's choice to terminate a pregnancy is a personal privacy right that is "implicit in the concept of ordered liberty,"[183] and that the government cannot interfere with that choice before the fetus is viable.[184] Specifically, *Roe* summarized the new constitutional rights of pregnant people during each trimester of pregnancy: (1) during the first trimester, any abortion regulations are plainly unconstitutional and the decision or procedure must be "left to the medical judgment of the pregnant [person's] attending physician;" (2) during the second semester, any abortion restrictions must be in the interest of promoting the pregnant person's health and must regulate the procedure in a way that is reasonably related to that interest; and (3) during the third trimester, the government can go so far as to ban abortion, as long as there is an exception to preserve the pregnant person's life or health.[185]

Almost twenty years after *Roe*, the Supreme Court decided *Planned Parenthood v. Casey*, in which it held that a state abortion

---

[179] CPCs are not required to follow HIPAA rules because they are not real medical providers. *What are Crisis Pregnancy Centers?*, *supra* note 154; Murphy, *supra* note 135.

[180] Murphy, *supra* note 135.

[181] Roe v. Wade, 410 U.S. 113, 152–53 (1973).

[182] *Id*. at 117–18.

[183] *Id*. at 152 (quoting Palko v. Connecticut, 302 U.S. 319, 325 (1937)).

[184] *Id*. at 163–64. Viability is usually placed at about seven months (twenty-eight weeks) but may occur earlier, even at twenty-four weeks. *Id*. at 160.

[185] *Id*. at 164–65.

regulation is only unconstitutional when it unduly burdens one's decision to have an abortion.[186] The Court replaced the trimester scheme used in *Roe* with the "undue burden" standard, which characterizes "state regulation[s with] the purpose or effect of placing a substantial obstacle in the path of a woman seeking an abortion of a nonviable fetus."[187] After *Casey*, it was constitutionally permissible for a state to regulate abortion during the first and second trimesters in the interest of parental or fetal health so long as it did not unduly burden one's right to choose.[188] While *Casey* chipped away at *Roe* by making it easier for states to restrict abortion, *Dobbs v. Jackson Women's Health* gutted the constitutional right to access abortion altogether.[189]

In *Dobbs*, the sole abortion provider in Mississippi, Jackson Women's Health Organization, sued the state's health officer Thomas Dobbs, claiming that the Mississippi Gestational Age Act unduly burdened abortion access and was therefore unconstitutional.[190] The Court did not decide the issue by applying the undue burden standard, but rather overturned *Roe* and *Casey* altogether and returned abortion regulation to the states.[191] It reasoned that "[t]he Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision," the doctrine of stare decisis does not mandate adherence to "*Roe*'s abuse of judicial authority," and *Roe* was "egregiously wrong from the start."[192] When it returned abortion regulation authority to the states, the Court ignored that the right to be free from unwelcomed government intrusion in personal and familial

---

[186] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 874, (1992).

[187] *Id*. at 873, 877.

[188] *Id*. at 877. The court upheld the existing standard that in the third trimester, the government can ban abortion with an exception for when the pregnant person's life is at risk. Roe, 410 U.S. at 164–65.

[189] *See* Dobbs v. Jackson Women's Health Org., 142 S.Ct. 2242, 2318 (2022).

[190] *Id.* at 2244. The Mississippi state law prohibited abortions after fifteen weeks of pregnancy, except in cases of severe fatal abnormalities or medical emergencies. *Id*.

[191] *See id.* at 2279.

[192] *Id.* at 2243.

decisions is both a constitutionally protected right and a fundamentally American principle.[193]

While the constitutional right to privacy and data privacy governance are separate issues operating under separate legal schemes, the underlying value is the same: an individual's interest in being left alone. *Dobbs* pushed the lack of comprehensive data protection laws into the spotlight[194] and emboldened anti-choice activists in their crusade against abortion rights, making it even more dangerous for individuals seeking reproductive healthcare.[195] One anti-choice proponent exclaimed, "[i]n a post-*Roe* world, our work [advocating against abortion] really begins in a lot of ways."[196] Given the nation's weak data privacy legal infrastructure and society's constant digitalization, anti-choice advocates will continue turning to exploitative data practices to further their message.

After the Court decided *Dobbs*, President Biden issued an Executive Order ("the Order") to promote access to reproductive healthcare.[197] In the Order, President Biden announced directives to combat data privacy threats, including tasking HHS with educating consumers on non-medical data privacy.[198] However, HHS had already issued two guidance documents in response to *Dobbs*.[199]

---

[193] *See, e.g.,* Griswold v. Connecticut, 381 U.S. 479, 485–86; Lawrence v. Texas, 539 U.S. 558, 562; Obergefell v. Hodges, 576 U.S. 644, 666; *see generally* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340 (1992).

[194] Jay Edelson, *Post-Dobbs, Your Private Data Will Be Used Against You*, BLOOMBERG LAW (Sept. 22, 2022), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you.

[195] Cott et al., *supra* note 156.

[196] *Id*.

[197] Exec. Order No. 14076, 87 Fed. Reg. 42053 (July 8, 2022).

[198] *Id*. This order aligns with HHS' mission to "enhance the health and well-being of all Americans" by providing them with accurate information about their legal rights in healthcare. *Introduction: About HHS*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/about/strategic-plan/2022-2026/introduction/index.html.

[199] *See Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, *supra* note 6; *see also HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, U.S. DEP'T HEALTH & HUM. SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/ phi-reproductive-health/index.html.

The first document explained the conditions under which HIPAA keeps reproductive health information private.[200] HHS provided a useful hypothetical: a law enforcement officer requests abortion procedure records from a health clinic without a court order or other legal mandate.[201] Under HIPAA, the healthcare provider cannot produce such records because it would entail releasing confidential personal health information without patient authorization.[202]

The second HHS guidance document addressed the post-*Dobbs* data privacy risks. HHS stated that managing one's own data privacy by not downloading "unnecessary apps" and turning off location services helps consumers protect themselves against "potential discrimination, identity theft, or harm to [their] reputation."[203] Discrimination, identity theft, and reputational harm are serious consequences, but *Dobbs* poses more grave threats, like surveillance and abortion criminalization.[204] These suggestions are infeasible because the majority of consumers understandably have hardly any understanding of data privacy concepts or laws.[205] Most uselessly, HHS advised individuals to "consider leaving the device at home."[206]

Unlike HHS, the FTC has more adequately responded to the Order's call to action by increasing its focus on protecting reproductive healthcare privacy.[207] In August 2022, the FTC commenced an enforcement action against the data broker Kochava, alleging that it collects and sells geolocation data on reproductive healthcare-related areas in violation of Section 5(a) of the FTC

---

[200] *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, *supra* note 199.

[201] *Id*.

[202] *Id*.

[203] *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, *supra* note 6.

[204] *See* Henson, *supra* note 27.

[205] A 2019 study found that fifty-nine percent of Americans understand "very little or nothing" about what companies do with data they collect, and sixty-three percent of Americans have "very little or no" knowledge on data privacy law. Auxier, *supra* note 9.

[206] *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, *supra* note 6.

[207] Exec. Order No. 14076, *supra* note 197; *see* Complaint at 1, F.T.C. v. Kochava, Inc., No. 2:22-CV-377 (D. Idaho filed Aug. 29, 2022).

Act.[208] The suit seeks injunctive relief that would bar Kochava from collecting and selling geolocation data related to sensitive locations like reproductive health clinics.[209] If this case continues to be fiercely litigated, it will show whether the Commission takes seriously its role as a data privacy rights enforcer.

The FTC's suit against Kochava is a step in the right direction for reproductive data privacy, but because *Dobbs* astronomically raised the stakes of privacy intrusions, the FTC's work alone is not enough.[210] *Dobbs* sparked national panic amongst citizens, prompting users across the country to delete fertility and period tracking apps[211] out of fear that their data would be used as evidence in states that are expected to criminalize abortion.[212] Most importantly, however, "trigger laws" that severely restrict abortion access became effective immediately after the Court released its decision.[213] One of the nation's most dystopian and frightening post-

---

[208] Complaint at 1, F.T.C. v. Kochava, Inc., No. 2:22-CV-377 (D. Idaho filed Aug. 29, 2022).

[209] *Id*. at 11. This case is currently in the pleadings stage.

[210] *See* Kade Crockford & Nathan Freed Wessler, *Impending Threat of Abortion Criminalization Brings New Urgency to the Fight for Digital Privacy*, ACLU (May 17, 2022), https://www.aclu.org/news/privacy-technology/impending-threat-of-abortion-criminalization-brings-new-urgency-to-the-fight-for-digital-privacy.

[211] Garamvolgyi, *supra* note 5. For those who still wish to use cycle tracking apps, Consumer Reports recommends the Drip, Euki, and Periodical apps because they "store data locally and don't allow third-party tracking." Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found.*, CONSUMER REPORTS (updated Aug. 30, 2022), https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a22781
34145/#:~:text=Overall%2C%20we%20recommend%20three%20of,researcher%20in%20CR's%20Digital%20Lab.

[212] States may now criminalize abortion procedures, because *Dobbs* returned abortion regulation to the states. *See* Henson, *supra* note 27.

[213] Before *Dobbs*, thirteen states had passed abortion bans that were challenged in court. When *Dobbs* overturned *Roe*, those challenges were effectively moot and the abortion bans were "triggered" to take effect. Elizabeth Nash & Isabel Guarnieri, *13 States Have Abortion Trigger Bans – Here's What Happens When Roe is Overturned*, GUTTMACHER INST. (June 6, 2022), https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned.

Dobbs trigger laws is the Texas Heartbeat Act, otherwise known as Senate Bill 8 ("S.B. 8").[214] S.B. 8 prohibits abortions once doctors detect a fetal heartbeat, which can happen as early as six weeks after conception.[215] This is particularly concerning because many individuals do not even suspect they are pregnant until after six weeks of gestation.[216] Thus, by the time some individuals suspect and confirm they are pregnant, it may be too late to have an abortion in compliance with S.B. 8.[217] Additionally, S.B. 8 grants individuals a private right of action to file civil enforcement suits against those who perform, assist, or intend to perform or assist illegal abortions.[218] Notably, the private right of action does not authorize individuals to sue the abortion patients themselves.[219] Plaintiffs may seek injunctive relief to prevent the abortion from happening or statutory damages "in an amount of not less than $10,000 for each abortion that the defendant performed" or assisted in performing.[220]

S.B. 8's private right of action is ostensibly a bounty hunter privilege that promotes vigilantism and is antithetical to the

---

[214] *See* TEX. HEALTH & SAFETY CODE ANN. § 171.204 (West 2021).

[215] *Id*.; Kelly Zielinski, *The Implication of Texas Abortion Law SB8 on at-Risk Populations in Texas and Other States*, 23 DEPAUL J. HEALTH CARE L. 52, 62–63 (2022).

[216] Individuals may not suspect they are pregnant until after six weeks of gestation if they experience irregular periods, do not plan to get pregnant, have hormone-related medical conditions, or lack proper sexual education. Jessica Ravitz, *Reasons a Woman May Not Know She's Pregnant at Six Weeks*, CNN (May 9, 2019), https://www.cnn.com/2019/05/09/health/pregnancy-at-six-weeks; Zielinski, *supra* note 220, at 63.

[217] A study by UCSF found that "one in three people confirm their pregnancies past six weeks, and one in five past 7 weeks." *One in Three People Learn They're Pregnant Past Six Weeks' Gestation*, ANSIRH (Nov. 10, 2021), https://www.ansirh.org/research/research/one-three-people-learn-theyre-pregnant-past-six-weeks-gestation; Zielinski, *supra* note 215, at 63.

[218] Any person, "other than an officer or employee of a state or local governmental entity in [Texas]" may bring a civil action under S.B.8. TEX. HEALTH & SAFETY CODE ANN. § 171.208 (West 2021).

[219] *See id*.; Zielinski, *supra* note 215, at 63.

[220] The damages award incentivizes individuals to enforce this law and the private right of action offers an enforcement mechanism. TEX. HEALTH & SAFETY CODE ANN. § 171.208(b)(1)–(2) (West 2021).

American judicial establishment.[221] This enforcement mechanism is particularly dangerous when considering the lack of a comprehensive federal data privacy law. For instance, consider an anti-choice man who learns that his newly pregnant neighbor plans to get an abortion from Alamo Women's Clinic.[222] The man might buy geolocation information from a data broker and learn that his neighbor's device was tagged at the clinic during her initial consultation. The man could then use this data as evidence in an S.B. 8 lawsuit to prevent the doctor from performing his neighbor's abortion.[223] Now, under *Dobbs*, S.B. 8 is a constitutionally compliant abortion law and serves as a model for other ultra-conservative anti-choice states.[224]

Data service providers, more so than anti-choice individuals, are in an optimal position to bring civil actions under S.B. 8 because they already "collect massive amounts of very personal data about individual pregnant people."[225] For example, FEMM is marketed as a mobile app that helps users meet their health goals by collecting information on sexual, menstrual, and hormonal health.[226] In the app, a user can indicate whether she had unprotected sex, if her period came late, or if she received a positive pregnancy test result.[227] On its face, FEMM appears neutral and does not advocate

---

[221] Zielinski, *supra* note 215, at 63; *see also* Kelly D. Hine, *Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck?*, 47 AM. U. L. REV. 1221, 1227 (1998).

[222] ALAMO WOMEN'S CLINIC (last visited Mar. 13, 2023), https://alamowomensclinic.com/.

[223] *See generally* Zielinski, *supra* note 215.

[224] *See* JOANNA R. LAMPE, CONG. RSCH. SERV., LSB10668, TEXAS HEARTBEAT ACT (S.B.8) LITIGATION: SUPREME COURT IDENTIFIES NARROW PATH FOR CHALLENGES TO TEXAS ABORTION LAW (2021); *Memo: Fifteen States and Counting Poised to Copy Texas' Abortion Ban*, NARAL, https://www.prochoiceamerica.org/report/memo-fifteen-states-and-counting-poised-to-copy-texas-abortion-ban/ (last visited Feb. 20, 2023).

[225] Cott et al., *supra* note 156.

[226] FEMM, https://femmhealth.org/get-started/ (last visited Mar. 13, 2023).

[227] FEMM, https://femmhealth.org/wp-content/uploads/2020/05/How-to-Use-the-FEMM-App-Final.pdf (last visited Mar. 18, 2023).

for or against abortion,[228] but the company has actually received $1.79 million[229] in funding from the Chiaroscuro Foundation, an anti-abortion and anti-contraception organization.[230] Thus, FEMM is at a huge advantage to breach user privacy and rely on the reproductive health-related data users provide it to bring civil suits against abortion providers under S.B. 8 to further its anti-choice values.

V. ENACTING A COMPREHENSIVE FEDERAL DATA PRIVACY STATUTE

Because *Dobbs* exacerbated an existing issue of privacy abuses, Congress must enact a comprehensive data privacy law to protect individuals' non-medical data from exploitation. This law must forbid entities from collecting consumer data without their knowledge, allow consumers to control what happens with their data, and afford consumers an opportunity to seek justice when their data privacy rights have been violated. Fortunately, a proposed federal statute meets these expectations.

In July 2022, the House Energy & Commerce Committee advanced a comprehensive data privacy bill called the American Data Privacy and Protection Act ("ADPPA").[231] This bipartisan bill would cure the patchwork privacy legal landscape by preempting

---

[228] Jessica Glenza, *Revealed: Women's Fertility App is Funded by Anti-Abortion Campaigners*, THE GUARDIAN (May 30, 2019, 2:00 AM), https://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners.

[229] FEMM was launched in 2015. FEMM's 2016, 2017, and 2018 IRS reports reveal the Chiaroscuro Foundation's contributions. *Id*.

[230] Sean Fieler is nearly the sole contributor to the Chiaroscuro Foundation and is a board member of the FEMM Foundation. In 2010–2014, Fieler contributed eighteen million dollars to anti-choice and anti-LGBTQ political campaigns. Amanda Arnold, *Popular Fertility App Funded by Anti-Abortion, Anti-Contraception Charity*, THE CUT (May 30, 2019), https://www.thecut.com/2019/05/fem-fertility-app-funded-by-anti-abortion-group-sean-fieler.html.

[231] JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (2022).

the existing state comprehensive privacy laws.[232] Four of the ADPPA's principals are noteworthy when viewing consumer data privacy through a reproductive healthcare lens—transparency, control, minimization, and enforcement.[233]

a. Transparency and Control

The ADPPA requires businesses and non-profit organizations ("Covered Entities") to disclose to consumers what type of data they collect, why they collect it, and for how long they retain it.[234] This notice requirement can help consumers make informed decisions, including whether to grant a service provider access to their personal data. Similar to the CCPA, the ADPPA grants consumers the rights to access, correct, and delete their data that has been collected by a Covered Entity.[235] The law also requires Covered Entities to obtain consumer consent before transferring their data to a third party, allowing for consumer data autonomy.[236] The ADPPA even addresses targeted advertising by granting consumers a right to withdraw themselves from the marketing tactic.[237] Before pushing targeted ads, a Covered Entity must provide the consumer with a "clear and conspicuous means to opt out of targeted advertising."[238] This creates a middle ground for consumers who enjoy targeted advertising's benefits and alternatively, those who do not want their data used for that purpose.

If Congress had passed the ADPPA before John Flynn began his anti-abortion geofencing campaign, the statute's transparency and control provisions would have sufficiently protected targeted consumers. The law would have required Flynn to notify the individuals he tagged at Planned Parenthood that he collected their geolocation data and explain why he collected it. Additionally, Flynn would have needed permission to transfer the individuals'

---

[232] *See id*.

[233] *See id*.

[234] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 202 (2022).

[235] *Id*. at § 203.

[236] *Id*. at § 204.

[237] *Id*. at § 204(c).

[238] *Id*. at § 204(c)(1)(A).

data to the anti-choice groups who paid him to geofence abortion clinics.

While this component of the proposed statute is a step in the right direction, Congress should make its targeted advertising provisions even more protective with respect to healthcare-related advertisements. The ADPPA should require Covered Entities pushing health or treatment-related targeted ads to offer consumers an opt-in selection. That way, consumers are presumed to be opted-out and would actively have to choose to receive health-related targeted advertisements. Thus, individuals would not receive undesired targeted advertisements unless they consented to their data being transferred for that purpose. For instance, individuals like those targeted by John Flynn would not have to navigate the opt-out technology behind targeted advertising—if they did nothing, they would not receive anti-choice ads. Shifting the burden of consumer protection to Covered Entities ensures that no individual would be subjected to unsolicited health-related targeted advertisements.

b. Minimization

The ADPPA includes a data minimization requirement, which prohibits Covered Entities from collecting, using, or transferring "sensitive data" that is beyond what is reasonably necessary to provide the consumer service.[239] Sensitive data includes a variety of personal information, like "precise geolocation" and "any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual."[240] This provision is essential to protecting abortion patients' privacy because geolocation, purchase pattern, and search history data can infer whether an individual has procured or considered an abortion procedure. For example, if the ADPPA had already been enacted, John Flynn's geofencing practices would violate the statute because the information likely reveals the individuals' healthcare treatment or condition. Similarly, FloHealth's practice of disclosing user

---

[239] *Id*. at § 101(a).

[240] *Id*. at §§ 2(28)(A)(ii), 2(28)(A)(vi), 102(2).

health-related data to third parties might have violated the ADPPA, if it disclosed data beyond what was needed to provide app services.

c. Enforcement

The ADPPA's enforcement mechanisms empower state attorneys general, individuals, and the FTC to seek justice for data privacy intrusions.[241] First, the statute permits state attorneys general to initiate civil actions against Covered Entities if there is "reason to believe that an interest of the residents of that State has been, may be, or is adversely affected by a violation of this Act."[242] Next, the ADPPA grants consumers a private right of action to sue Covered Entities directly for equitable relief or damages.[243] Finally, it authorizes the FTC to bring civil actions against Covered Entities who violate the statute.[244] The ADPPA even creates a new FTC bureau, the Bureau of Privacy, specifically to handle data privacy violations and enforcement actions.[245] Currently, the FTC's Bureau of Consumer Protection handles most data privacy issues.[246]

The Bureau of Privacy is intended to function[247] as the existing FTC bureaus do: it would investigate potential FTC Act violators, engage in rulemaking proceedings,[248] and carry out enforcement actions.[249] This bureau is necessary because of consumers' inability to identify when their data privacy rights are violated by third parties. For instance, if a consumer does not receive proper notice

---

[241] *Id*. at §§ 401–403.

[242] *Id*. at § 402.

[243] *Id*. at § 403.

[244] *Id*. at § 401.

[245] *Id*.

[246] *See About the Bureau of Consumer Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection (last visited Mar. 13, 2023).

[247] *See* H.R. 8152, 117th Cong. § 401(a)(1).

[248] "Often, when Congress passes a law . . . some of the details may need to be filled in. The law may tell an agency to fill in those details with a rule. This process is called agency rulemaking, and it results in final rules that become federal law." *Public Participation in the Rulemaking Process*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/rulemaking/public-participation-rulemaking-process (last visited Feb. 20, 2023).

[249] *See About the Bureau of Consumer Protection*, *supra* note 246.

that an entity transferred her data to a third party, she would be unaware that an entity has violated her rights under the ADPPA. Thus, that consumer would not know that she has grounds to bring a private action. The Bureau of Privacy would mend the enforcement gap left by the private right of action by proactively investigating Covered Entities on consumers' behalf. These three enforcement mechanisms make the ADPPA a stringent, comprehensive data law that can adequately protect against privacy violations in reproductive healthcare settings. Ultimately, the ADPPA will create a cohesive legal doctrine that grants consumers critical privacy rights.

CONCLUSION

Data privacy is underregulated in the United States, allowing anti-choice parties to abuse and exploit individuals' non-medical data. The threat of abortion criminalization and data surveillance post-*Dobbs* requires a swift legislative response. Currently, the fragmented data privacy legal landscape is insufficient to protect consumers from data abuse that can carry life-changing consequences. To curtail the data privacy-related risks that abortion patients face, Congress must enact a refined version of the ADPPA that enhances protections against healthcare related targeted advertising by presuming that consumers are opted-out of receiving them. The solution is not—and cannot be—making Americans leave their phones at home.