

CONTROLLED CONSENT: A BLOCKCHAIN SOLUTION TO UNCERTAIN REPRODUCTIVE RIGHTS

*Jacob A. Williams**

I. INTRODUCTION

Sarah's heart races as she reads the email on her smartphone: URGENT: Potential Data Breach Notification. In compliance with the Federal Trade Commission's Health Breach Notification Rule,¹ we regret to inform you that your personal health records may have been compromised in a recent security incident. The words blur as Sarah's mind races. Her period tracking app, the one she has faithfully used for years, now feels like an unwelcome visitor in her personal life. She thinks of the data stored in the app: her cycle predictions, the symptoms she's logged, and even the dates she's marked for doctor's appointments. In the wrong hands, this information could lead to more than just embarrassment; it could have serious consequences in a legal landscape increasingly divided on reproductive freedom. As she scrolls through the email, a thought nags at her: "Was using this app a huge mistake?"

In 2021, Flo, an app that advertises itself as the "#1 Women's Health App,"² came under scrutiny for breaches of its privacy policy after deceptively selling user data.³ The Federal Trade Commission ("FTC") investigated Flo and similar apps, finding their development teams responsible for sharing the sensitive health data of millions of users with marketing giants like Facebook and Google.⁴ These transactions enabled the data recipients to cultivate targeted advertisements to app-users based on information those users thought was private.⁵ These breaches are

*J.D. Candidate, Northern Kentucky University Salmon P. Chase College of Law, 2026; Bachelor of Arts in Economics, Maryville College, 2019. I would like to thank my supervising professor, Michelle Browning-Coughlin, my senior editor, Nathan Thacker, and the other editors of the Northern Kentucky Law Review for their resourceful advice and guidance throughout this project. Lastly, I am forever grateful for my family's encouragement and support throughout my legal journey.

¹16 C.F.R. § 318 (2023).

²Flo Health, Flo, <https://flo.health/> (last visited Oct. 27, 2024).

³FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, 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>.

⁴*Id.*

⁵Press Release, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order, Fed. Trade Comm'n (May 17, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>.

especially impactful to women seeking reproductive healthcare information, a population now at risk of having routine health data subpoenaed as evidence in a lawsuit or state investigation where strict abortion laws are present.⁶

Traditional data privacy protections—password security or discrete data entry—cannot secure a woman’s online safety when companies are actively breaching privacy policies in violation of their own agreements. However, by enabling a user to limit the information stored in data-related transactions, blockchain technology offers a transformative solution. By empowering users to better control their own health data and who has access to it, blockchain could safeguard sensitive information from being sold or misused without the required consent or immediate notice of the relevant party.⁷

This Note asserts that implementing and regulating a blockchain-based system for individualized reproductive health data management offers a potential solution to privacy challenges faced by women in the United States. To explore this proposition, Section II of the article will outline the shifting tides of recent reproductive health challenges, focusing on Texas as an example of a state with strict abortion legislation.⁸ Section III will explain the relevant technology behind blockchain: cryptography, hashing, immutability, and decentralization.⁹ Finally, Section IV synthesizes these concepts, evaluating the strengths of moving to a blockchain system for reproductive health data management, while also addressing potential challenges and their implications.¹⁰

II. VULNERABLE DATA IN A PATCHWORK LEGAL LANDSCAPE

Sarah’s hypothetical scenario in the introduction illustrates a growing concern in today’s legal and technological landscape: the vulnerability of personal health records (“PHRs”) in a post-*Dobbs* nation.¹¹ Unlike records protected by the Health Insurance Portability and Accountability Act (“HIPAA”), PHRs are governed by a patchwork of regulations encompassing consumer protections and privacy legislation.¹² This patchwork, while comprehensive in scope, leaves PHRs vulnerable to

⁶ *Id.* (Consumers felt “outraged,” “victimized,” and “violated.”)

⁷ See Chad Anderson et al., *Blockchain Innovation for Consent Self-Management in Health Information Exchanges*, 174 DECISION SUPPORT SYS., Nov. 2023, at 1, 6.

⁸ See *infra* p. 9.

⁹ See *infra* p. 16.

¹⁰ See *infra* p. 22.

¹¹ Press Release, *HHS Issues Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe*, U.S. DEP’T OF HEALTH & HUMAN SERVS. (June 29, 2022), <https://www.hhs.gov/about/news/2022/06/29/hhs-issues-guidance-to-protect-patient-privacy-in-wake-of-supreme-court-decision-on-ro.html>.

¹² *Id.*

potential misuse.¹³ The FTC's Health Breach Notification Rule, revised on July 29, 2024, aims to address the gaps by requiring companies that process PHRs to promptly report potential breaches to at-risk consumers and the FTC within a set time frame.¹⁴ However, limited safeguards alone cannot fully protect PHRs pertinent to abortion access in a nation where abortion regulation varies dramatically from state to state. The seminal decision in *Dobbs v. Jackson Women's Health Organization*,¹⁵ which overturned *Roe v. Wade*,¹⁶ has raised questions about the legal implications of sharing health data in states with restrictive abortion policies.

In this fragmented landscape, data collected by wearable devices, apps, and trackers such as location, daily routines, and even spending habits can be easily weaponized in court proceedings.¹⁷ Without clear protections or consistent privacy standards, women face legal consequences based on data they unknowingly expose.¹⁸ The urgency for more secure, user-controlled systems for electronic health records under HIPAA, is undeniable.¹⁹ The Health Information Technology for Economic and Clinical Health Act, or HITECH Act, is just one signal that this need has been recognized in healthcare.²⁰ Extending these principles to PHRs through innovative technologies like blockchain could offer a path forward, enabling individuals to control their data whilst shielding them from misuse in an environment that is increasingly hostile to reproductive rights. Fictional in name only, Sarah's circumstances highlight the urgent need for more robust, user-controlled methods of managing personal health records.

¹³ See *id.*

¹⁴ Press Release, *FTC Finalizes Changes to the Health Breach Notification Rule*, FED. TRADE COMM'N (Apr. 26, 2024) (on file with author) (The rule allows a 60-day period for notification concerning breaches where 500 or more users may have been affected, and a 60-day period starting from the end of the year for breaches where fewer than 500 users may have been impacted).

¹⁵ *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022).

¹⁶ *Roe v. Wade*, 410 U.S. 113 (1973), *overruled by Dobbs*, 597 U.S. at 268-69.

¹⁷ Jessica Taylor-Price, *A woman's Facebook Messages Were Used in an Abortion Case. Here's Why That's Not Surprising*, NE. GLOBAL NEWS (Aug. 18, 2022), <https://news.northeastern.edu/2022/08/18/facebook-data-abortion/>.

¹⁸ *Id.*

¹⁹ See Müge Fazlioglu, *Filling the void? The 2023 State Privacy Laws and Consumer Health Data*, INT'L ASS'N OF PRIV. PROF'LS (Mar. 28, 2023), <https://iapp.org/news/a/filling-the-void-the-2023-state-privacy-laws-and-consumer-health-data> (noting that limitations in the scope of the Health Insurance Portability and Accountability Act, a broad array of data, such as that collected by mobile devices, apps or wearable fitness trackers, has remained outside the law's reach).

²⁰ Steve Adler, *What is the HITECH Act?*, HIPAA J. (Jan. 11, 2024), <https://www.hipaajournal.com/what-is-the-hitech-act/#whatarethegoalsofthehitechact> (noting that the goals of the HITECH Act are to (1) Improve quality, safety, and efficiency, (2) Engage patients in their care, (3) Increase coordination of care, (4) Improve the health status of the population, and (5) Ensure privacy and security).

With the spotlight on the risks of current health data management systems, emerging technologies like blockchain offer promising solutions to protect sensitive reproductive health information. The backbone of cryptocurrencies like Bitcoin and Ethereum,²¹ blockchain technology is poised to revolutionize healthcare by offering unprecedented data security, and, in turn, a degree of patient empowerment.²² Originating in the security-driven world of financial technology, blockchain creates an immutable, decentralized ledger of transactions.²³ In healthcare, this could translate to a financial concept akin to a “data wallet,” used to store individual cryptocurrency or important financial information.²⁴ The digital file could enable users to store and selectively share critical health information, such as aforementioned period tracking data or information regarding medical visits, while ensuring privacy from unauthorized parties.²⁵ For women navigating reproductive healthcare, this technology could serve as a data buffer, shielding them from the potential misuse of personal data in states with restrictive laws. More importantly, it would provide them with an added level of consent when choosing to share PHRs.²⁶

However, implementing blockchain in a healthcare system comes with challenges. Widespread adoption requires overcoming significant barriers, including limited public understanding of the technology, ensuring equitable access, and regulating a commercialized data market reliant on data transfer for its efficiency.²⁷ Policymakers, along with dedicated technologists, must ensure that blockchain systems enhance, rather than undermine, the legal protections for reproductive health information. Trialing a system of this kind without proper security measures in place leaves users with the same vulnerabilities they are already exposed to.²⁸ Transparency and ethical considerations must remain central to

²¹ Ewan Lewis, *What Is Blockchain: The Backbone of Cryptocurrency*, DAILYCOIN (July 24, 2024, 12:00 PM GMT) <https://dailycoin.com/what-is-blockchain-backbone-of-cryptocurrency/>.

²² See generally Ashutosh Dhar Dwivedi et al., *A Decentralized Privacy-Preserving Healthcare Blockchain for IoT*, 19 SENSORS, 326 (2019).

²³ Lewis, *supra* note 21, at 3.

²⁴ Massimo Artoressi, *Digital identity wallet*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/digital-identity-wallet_en (last visited Nov. 24, 2024).

²⁵ See generally Alexandra Cernian et al., *Patient Data Chain: A Blockchain-Based Approach to Integrate Personal Health Records*, NAT’L LIBR. OF MED. – SENSORS (2020), [sensors-20-06538-v2.pdf](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC705338/) (noting that Blockchain technology eliminates the need for numerous “transactions” within a single doctor’s visit).

²⁶ *Id.*

²⁷ Bill Genovese, *Blockchain Technology: Hype or Reality?*, CIO (Apr. 22, 2016), <https://www.cio.com/article/240856/blockchain-technology-hype-or-reality.html>.

²⁸ See generally Meredith Somers, *The Risks and Unintended Consequences of Blockchain*, MIT SLOAN SCH. OF MGMT. (July 18, 2019), <https://mitsloan.mit.edu/ideas-made-to-matter/risks-and-unintended-consequences-blockchain> (noting that blockchain has advantages that can be misused without proper knowledge of how the system operates).

blockchain's development as well. The use of this technology is not intended to bypass legitimate law enforcement or abortion-limiting legislation, rather it is to help provide security to users regularly interfacing with apps that may disclose sensitive information. In turn, reducing unnecessary leaks of sensitive health data and empowering individuals providing informed consent.

This Note posits that the importance of protecting reproductive health data has only been magnified since *Dobbs*. This landmark decision not only reshaped the legal landscape of abortion access but amplified concerns about how personal health data could be weaponized in states with restrictive reproductive health legislation.²⁹

A. CTRL+ALT+DEL: A New Narrative in the Reproductive Health Landscape

In determining *Dobbs*, the Supreme Court grappled with the weighty implications of dismantling nearly fifty years of precedent that had embedded abortion rights into American constitutional law.³⁰ The case overturned *Roe v. Wade*³¹ and *Planned Parenthood of Southeastern Pennsylvania v. Casey*³² -- two cases that, while divisive in history, were instrumental in protecting a woman's right to elect terminating her own pregnancy. The majority opinion in *Dobbs*, written by Justice Alito, concluded that access to abortion was never a fundamental right within the constitution, and that the decision to legalize the act is best left to the states and their voters.³³ In their *Dobbs* dissent, Justices Breyer, Sotomayor, and Kagan emphasized the damaging ramifications this decision would have on women's rights.³⁴ They also warned about the potential impact on numerous precedents that had relied on the now overturned case law.³⁵

At the time that *Roe* was overturned, thirteen states had "trigger laws" waiting to take effect, resulting in a total ban of abortions in some states.³⁶ Several of these state laws do not include exceptions in even the most severe

²⁹ Price, *supra* note 17, at 3.

³⁰ See generally *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022) (where the Court is clearly at odds over such a prominent challenge to *stare decisis* and articulates the complexity of the future of abortion law).

³¹ See *Roe v. Wade*, 410 U.S. 113 (1973), *overruled by Dobbs*, 597 U.S. at 268-69. (establishing a constitutional right to privacy in reproductive healthcare options).

³² See generally *Planned Parenthood of Se. Pennsylvania v. Casey*, 505 U.S.833 (1992) (establishing that state regulations on abortion are unconstitutional if they impose an "undue burden" on a woman's right to terminate her pregnancy before viability), *overruled by Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022).

³³ See *Dobbs*, 597 U.S. at 256.

³⁴ *Id.* at 362-417 (Breyer, Sotomayor & Kagan, JJ., dissenting).

³⁵ *Id.*

³⁶ See *After Roe Fell: Abortion Laws by State*, CENTER FOR REPRODUCTIVE RIGHTS, <https://reproductiverights.org/maps/abortion-laws-by-state/> (last visited Nov. 24, 2024).

circumstances, such as rape or incest.³⁷ This presents a cold contrast for a formerly recognized fundamental right, quite literally vanishing overnight.³⁸ These strict provisions have highlighted fundamental tensions between state regulatory power and established medical ethics guidelines regarding patient care in traumatic circumstances.³⁹ In response to this legal shift, states have moved in opposing directions—some implementing near-total abortion bans with others codifying abortion protections into state law—creating a patchwork of regulations across the country.⁴⁰

In this fragmented aftermath, legal challenges to new abortion-related policies have rapidly emerged. Texas serves as a particularly informative case study on the early nature of extreme, abortion-related lawsuits, revealing two significant data trends in reproductive health access. First, state-level data show a dramatic decline in reproductive healthcare services right after the *Dobbs* decision.⁴¹ This trend likely underlines significant new barriers to accessing reproductive care or a general fear on how to aid in or report these operations.⁴²

The second notable trend appears in out-of-state data, which reveal an unprecedented increase in reproductive health visits in states without abortion bans, particularly those adjacent to states with restrictive legislation.⁴³ This trend likely represents that people are crossing state lines to receive reproductive health care.⁴⁴ Justice Kavanaugh addressed this potential consequence in his concurrence in *Dobbs*.⁴⁵ He stated that the constitution was neutral on the issue of abortion and reasoned that a state could not ban its citizens from traveling to receive abortions in a state where the service is legal.⁴⁶

This interstate travel question has already manifested in Texas courts, providing an early test of Justice Kavanaugh's analysis given the state's strict anti-abortion stance. In 2023, a man brought an action against his ex-wife's three friends for helping her receive an out-of-state abortion in

³⁷ *Id.*

³⁸ See Mabel Felix et al., *A Closer Look at Rape and Incest Exceptions in States with Abortion Bans and Early Gestational Restrictions*, KFF (Aug. 7, 2024), <https://www.kff.org/policy-watch/rape-incest-exceptions-abortion-bans-restrictions/>.

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ See *Texas Abortion Data: State Profiles for Women's Health*, KFF (July 29, 2024), <https://www.kff.org/interactive/womens-health-profiles/texas/abortion-statistics/>.

⁴² See generally *id.*

⁴³ See Molly C. Escobar et al., *171,000 Traveled for Abortions Last Year. See Where They Went*, N.Y. TIMES (June 13, 2024), <https://www.nytimes.com/interactive/2024/06/13/us/abortion-state-laws-ban-travel.html>.

⁴⁴ *Id.*

⁴⁵ See *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 346 (2022) (Kavanaugh, J., concurring).

⁴⁶ *Id.*

Colorado, directly challenging the boundaries of cross-border reproductive care.⁴⁷ While prominent anti-abortion lawyers quickly attached themselves to the case before its out-of-court settlement,⁴⁸ the incident underscores the pressing need to examine Texas's comprehensive statutory framework. In 2024, a data removal company, Atlas Privacy, demonstrated that organizations maintaining cooperative relationships with law enforcement could retain access to location data tracking individuals' devices as they traveled to out-of-state clinics.⁴⁹ As one of the most aggressive states in restricting abortion access, Texas's approach offers critical insights into how interstate abortion rights may be tested in the post-*Dobbs* era.

B. Trouble in Texas: Senate Bill 8 and Its Legal Aftermath

Texas has gained controversial notoriety due to a statute that enables what some critics call a “bounty system.”⁵⁰ Under Texas Health and Safety Code § 171.208(b)(2), the law empowers private citizens, excluding law enforcement, to file civil lawsuits against individuals who have received or aided in an abortion.⁵¹ Notably, the statute allows action only in cases where the mother's life is not in immediate danger, meaning no exceptions are made for instances of rape or incest.⁵² This law has drawn sharp criticism for circumventing traditional enforcement mechanisms and incentivizing private citizens to act as enforcers of abortion restrictions, adding a layer of complexity to the legal landscape surrounding abortion access.⁵³

Prior to *Dobbs*, Texas's Senate Bill 8 (“S.B. 8”), a comprehensive package of anti-abortion laws, faced a key pre-enforcement challenge. In *Whole Woman's Health v. Jackson*, a group of abortion providers and advocacy organizations sought to enjoin the law rather than waiting for it to

⁴⁷ *In re Brittni Silva*, No. 14-23-00834-CV, 2024 WL 1514565 (Tex. App., Apr. 9, 2024).

⁴⁸ Doha Madani, *Texas man sues ex-wife's friends, alleging they helped her get abortion pills in violation of state law*, NBC NEWS (Mar. 12, 2023), <https://www.nbcnews.com/news/us-news/texas-man-sues-ex-wifes-friends-allegedly-helping-get-abortion-pills-v-rcna74541>; see also *Texas man settles lawsuit against women accused of aiding in wrongful death by helping wife obtain abortion pill*, CBS TEXAS (Oct. 13, 2024, 11:59 AM), <https://www.msn.com/en-us/news/other/texas-man-settles-lawsuit-against-women-accused-of-aiding-in-wrongful-death-by-helping-wife-obtain-abortion-pills/ar-AA1sbTQ9?ocid=BingNewsSerp>.

⁴⁹ Lisa Femia, *Location Tracking Tools Endanger Abortion Access. Lawmakers Must Act Now.*, ELEC. FRONTIER FOUND. (Dec. 4, 2024), <https://www.eff.org/deeplinks/2024/12/location-tracking-tools-endanger-abortion-access-lawmakers-must-act-now>.

⁵⁰ E.g., Emma Bowman, *As states ban abortion, the Texas bounty law offers a way to survive legal challenges*, NPR (July 11, 2022, 5:00 AM), <https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law>.

⁵¹ See TEX. HEALTH & SAFETY CODE ANN., tit. 2, ch. 171.208 (2021).

⁵² *Id.*

⁵³ See Philip Elliot, *That Texas Abortion Case Is Even Worse Than You Think*, TIME (Dec. 15, 2023, 7:00 AM), <https://time.com/6510970/abortion-texas-case/>.

impact them in any way.⁵⁴ The plaintiffs were providers, nurses, and patients who argued that S.B. 8 would harm their ability to provide or adequately access care.⁵⁵ The defendants targeted were comprised of state officials sitting in their official capacity. The defendants in *Whole Woman's Health v. Jackson* included Judge Jackson of the 114th District Court and Clerk Clarkston who would process S.B. 8 lawsuits; executive officials with licensing and disciplinary authority over healthcare providers (Carlton of the Texas Medical Board, Thomas of the Nursing Board, Benz of the Pharmacy Board, and Young of Health and Human Services); Texas Attorney General Paxton who could potentially enforce penalties against physicians; and Mark Lee Dickson, a private citizen who had expressed intent to bring enforcement actions under S.B. 8.⁵⁶ All defendants moved to dismiss, citing both their sovereign immunity and the plaintiffs' failure to demonstrate grounds for relief beyond hypothetical damages.⁵⁷

The district court initially rejected the defendants' claims of immunity, finding persuasive the plaintiff's argument that judicial officials, and even private citizens, were not granted immunity because the plaintiffs were trying to prevent action, not remedy existing damages.⁵⁸ However, the case climbed to the Supreme Court, where the justices significantly narrowed the scope of possible defendants.⁵⁹ The Court unanimously rejected the petitioners' theory for relief against state-court judges and clerks, finding they were indeed protected by sovereign immunity because they merely adjudicate disputes, rather than enforcing laws.⁶⁰ The Court also dismissed claims against the Texas Attorney General and the private individual defendant, effectively gutting the plaintiffs' action.⁶¹

While *Whole Woman's Health* did not directly foreshadow the Supreme Court's *Dobbs* ruling, it was a precursor for the legal battle over state abortion laws. The Supreme Court allowed the case to proceed only against the medical licensing officials who had specific disciplinary authority over medical licensees.⁶² This narrow ruling preserved one pathway for federal pre-enforcement challenges to S.B. 8, while emphasizing that other avenues remained available, such as constitutional defenses following enforcement

⁵⁴ *Whole Women's Health v. Jackson*, 556 F. Supp. 3d 595, 602-03 (W.D. Tex.), *aff'd in part, rev'd in part, and remanded sub nom.* *Whole Woman's Health v. Jackson*, 595 U.S. 30 (2021).

⁵⁵ *Id.* at 606-07.

⁵⁶ *Id.* at 607-08.

⁵⁷ *Id.* at 613-14.

⁵⁸ *Id.* at 633.

⁵⁹ *Whole Woman's Health v. Jackson*, 595 U.S. 30, 252 (2021).

⁶⁰ *Id.* at 523 (explaining that usually, those individuals, state-court judges and clerks, do not enforce state laws like executive officials, rather, they work to resolve disputes between parties).

⁶¹ *Id.*

⁶² *Id.* (noting the petitioners' theories for relief also present some opportunities).

proceedings. The Court's decision may only have focused on the procedural questions regarding sovereign immunity and proper defendants; however, its eventual outcome arguably crippled avenues for challenging the enforcement of S.B. 8 itself.

The practical implications of S.B. 8 became apparent in 2021, when San Antonio-based doctor Alan Braid gained national media attention by publicly announcing that he had performed an abortion in violation of Texas's law.⁶³ Braid, who faced two lawsuits as a result, stated in an op-ed piece published by *The Washington Post* that the care he provided was consistent with his professional duty—medical care.⁶⁴ Oddly, the individuals who sued Dr. Braid stated they did not support Texas's abortion ban. One individual did not even live within the state but wanted the court to take up the topic of its constitutionality directly.⁶⁵ In what was believed to be a win for abortion rights at the time, the cases against Dr. Braid were dismissed on the theory that a bystander, a stranger to the case, did not have standing under Texas's law to sue absent showing actual harm to him or herself.⁶⁶

While Texas has been the front runner for abortion-restricting legislation, other states have developed model legislation in an attempt to define clear, albeit narrow, exceptions where an abortion is permitted.⁶⁷ As these laws continue to be tested in the courts, the broader implications for individuals seeking abortions extend beyond physically accessing care to include growing risks to their personal data. The intersection of these legal challenges and the collection of sensitive reproductive health data from apps, trackers, and medical providers has created a complex web of privacy vulnerabilities. With these shifting legal barriers and the potential for personal health information to be used against individuals in legal proceedings, the need for robust data privacy protections has never been more urgent.

⁶³ Alan Braid, *Why I violated Texas's extreme abortion ban*, WASH. POST (Sep. 18, 2021), <https://www.washingtonpost.com/opinions/2021/09/18/texas-abortion-provider-alan-braid/>.

⁶⁴ *Id.*

⁶⁵ See generally Tierney Sneed & Ariane De Vogue, *Texas doctor who says he performed abortion sued in first known challenges under new law*, CNN (Sep. 20, 2021, 10:36 PM), <https://www.cnn.com/2021/09/20/politics/texas-abortion-doctor-lawsuit/index.html>.

⁶⁶ Annie Gimbel, *Texas court dismisses case against Dr. Alan Braid for violating abortion ban*, CBS NEWS (Dec. 9, 2022, 9:52 AM), <https://www.cbsnews.com/texas/news/texas-court-dismisses-case-against-dr-alan-braid-violating-abortion-ban/>.

⁶⁷ Mabel Felix et al, *A Review of Exceptions in State Abortion Bans: Implications for the Provision of Abortion Services*, KFF (June 6, 2024), <https://www.kff.org/womens-health-policy/issue-brief/a-review-of-exceptions-in-state-abortions-bans-implications-for-the-provision-of-abortion-services/>.

C. Private Causes of Action Alongside Privacy Exploitation

A critical concern for individuals seeking abortion access in the United States is the protection of their health data privacy. The issue is complicated by a fragmented regulatory landscape where both federal and state laws govern personal data, and it is often unclear how those laws apply. It would not be out of character to think the combination of HIPAA and HITECH might cover healthcare data on apps, especially provided HITECH's data focus. However, period-trackers and wellness apps classified as consumer health apps do not fall within the scope of regulation surrounding this subject.⁶⁸ Data privacy matters, especially those involving PHRs, often instead fall within a strange gray area created between HIPAA and the FTC's consumer protection regulations.⁶⁹ Unlike the European Union's highly prescriptive GDPR, the U.S. lacks comprehensive federal data privacy legislation.⁷⁰ This regulatory landscape results in states having significant latitude in establishing additional privacy protections for their citizens.

In 2023, the FTC took significant enforcement actions demonstrating both the scale of health data misuse and the agency's renewed commitment to consumer protection. For example, online therapy platform BetterHelp agreed to a \$7.8 million settlement after sharing users' sensitive personal health information with social media platforms like Facebook, Snapchat, and Pinterest.⁷¹ The FTC alleged that BetterHelp disclosed email addresses, IP addresses, and health questionnaire information for advertising purposes despite promising consumers it would not use or disclose personal health data, except for limited purposes.⁷² According to the FTC's complaint, BetterHelp used consumers' email addresses and therapy history to instruct Facebook to identify similar consumers for targeted advertisements, which helped the company attract tens of thousands of new users, generating millions in revenue.⁷³

Similarly, GoodRx, a prescription pricing service, faced a \$1.5 million civil penalty for disclosing users' prescription information and health

⁶⁸ See Price, *supra* note 17.

⁶⁹ *Id.*

⁷⁰ See Connor Murray, *U.S. Data Privacy Protection Laws: A Comprehensive Guide*, FORBES (Apr. 21, 2023, 9:02 AM), <https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/>.

⁷¹ Press Release, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, FED. TRADE COMM'N (Mar. 2, 2024), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>.

⁷² *Id.*

⁷³ *Id.*

conditions to third-party advertisers, representing the FTC's first enforcement action under the Health Breach Notification Rule.⁷⁴ The FTC alleged that since 2017, GoodRx shared users' prescription medications and health conditions with advertising companies Facebook, Google, and Criteo, despite ensuring users it would never share this information.⁷⁵ The FTC has since clarified and strengthened this rule, explicitly stating that it applies to health apps and similar technologies not covered by HIPAA, and that the definition of "breach of security" includes data security breaches and unauthorized disclosures.⁷⁶

With increased scrutiny placed on women and their reproductive health options, understanding how existing data privacy practices enabled the exposure of confidential reproductive health records may be key to be preventing it in the future. Prominent health-tracking apps have repeatedly violated user trust: Flo Health shared fertility data with major retailers⁷⁷, Premom provided Chinese companies with user geolocation and device information⁷⁸, and other platforms have been implicated in unauthorized data sharing. The FTC finalized a settlement with Flo Health that required the company to obtain affirmative consent from users before sharing their personal health information and to notify affected users about previous unauthorized disclosures.⁷⁹

Since the complaint against Flo Health, FTC directives and media releases have become increasingly explicit about required consumer protections. Flo and similar apps have attempted remediation by identifying specific breach occurrences and implementing transparency measures.⁸⁰ Most notably, Flo introduced an "anonymous mode" enabling users to track reproductive cycles without entering personally identifiable information.⁸¹ While these steps toward transparency are noteworthy, they cannot fully mitigate the fundamental harm: users were targeted based on their personal

⁷⁴ Press Release, FTC Takes Enforcement Action Against GoodRx for Failing to Notify Consumers and Others of Unauthorized Disclosure of Personal Health Information, FED. TRADE COMM'N (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>.

⁷⁵ *Id.*

⁷⁶ Lesley Fair, *Updated FTC Health Breach Notification Rule puts new provisions in place to protect users of health apps and devices*, FED. TRADE COMM'N: BUS. BLOG (Apr. 26, 2024), <https://www.ftc.gov/business-guidance/blog/2024/04/updated-ftc-health-breach-notification-rule-puts-new-provisions-place-protect-users-health-apps>.

⁷⁷ *FTC Finalizes Order with Flo Health*, *supra* note 3.

⁷⁸ *Ovulation Tracking App Premom Will be Barred from Sharing Health Data*, *supra* note 5.

⁷⁹ *FTC Finalizes Order with Flo Health*, *supra* note 3.

⁸⁰ *Privacy Policy*, FLO HEALTH, <https://help.flo.health/hc/en-us/categories/360000883431-Privacy-Security> (last visited Dec. 3, 2024) While the lawsuit against Flo is mentioned on their privacy screen, no information pertaining to the settlement is discussed. *Id.*

⁸¹ *Id.*

circumstances through unlawful data sharing. The real danger lies in how these companies, as the FTC noted in its enforcement actions against both BetterHelp and GoodRx, allowed third parties to use sensitive health information for their own purposes, improving on advertising systems without placing meaningful limits on how intimate data could be used.⁸²

D. HIPAA's Digital Blindspot and Individual Privacy Needs

HIPAA was not designed to address the evolving concerns of modern data breaches. The law applies to “covered entities,” healthcare providers and their plans along with providers’ direct business associates.⁸³ This language, while broad, does not extend to apps like Flo where consumers are interacting with the apps directly instead of through a healthcare medium.⁸⁴ As a result, users of these apps are left without the robust privacy protections that HIPAA offers, relying instead on often vague company privacy policies and broad consumer protection laws. This gap has only expanded following the *Dobbs* decision because these data are now vulnerable to legal requests from states or independent parties looking to obtain records for evidentiary purposes.

In the absence of clear privacy protections, individuals navigating reproductive health choices in a post-*Dobbs* world face heightened risk. They are left questioning how they can protect themselves against unintended legal consequences stemming from the misuse of their health data occurring on apps. While the issues contested in Texas differ from those faced by Flo from a legal perspective, the two matters reduce an individual’s autonomy in choice and understood consequence.⁸⁵ Whether regarding the judiciary, a state legislature, or an app, questions persist about how individuals can better protect themselves against unintended legal consequences.⁸⁶

Readily tested in similar markets, blockchain transactions offer a versatility and structure necessary to protect sensitive data in a highly regulated environment. Blockchain provides secure, transparent, and user-controlled systems, which could offer the protection individuals need in today’s data-driven landscape.⁸⁷ Section III of this Note will explore how

⁸² *FTC Takes Enforcement Action Against GoodRx*, *supra* note 75.

⁸³ See Fazlioglu, *supra* note 19.

⁸⁴ *Id.*

⁸⁵ E.g., Timothy Gardner & Richard Webner, *Texas law sparks hundreds of U.S. protests against abortion restrictions*, REUTERS (Oct. 4, 2021), <https://www.reuters.com/world/us/abortion-rights-advocates-will-march-across-us-protest-restrictive-laws-2021-10-02/>.

⁸⁶ *Id.*

⁸⁷ See generally V. Malik et al., *Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based*

blockchain technology, with its security and fraud detection features, can provide a more reliable solution to the privacy challenges faced by users of reproductive health apps.

III. LOOKING BEYOND THE BUZZWORD: THE IMPLEMENTATION OF BLOCKCHAIN

Blockchain, established as a multi-disciplinary technology, has exploded in its implementation in biomedical settings in recent years.⁸⁸ While Bitcoin made blockchain an industry name, the foundational aspects of the technology have been around since the 1990s.⁸⁹ A “block” is a small digital transaction containing the necessary information of a needed to communicate, most often including party identifiers, a numerical or coded identifier specific to the transaction, and a timestamp.⁹⁰ These blocks formulate one after another, transaction by transaction, to create a chain of historical data.⁹¹ Transacting in this manner seeks to eliminate unnecessary middlemen, and their associated costs, by verifying an individual’s credentials and only allowing the transaction to proceed based on that verification.⁹² In this way, blockchain creates a *trustless* system, not reliant upon a medium or specific organization for its authorization.⁹³ The growing availability of the technology, its application in international settings, and its successful trialing in different industries makes it an increasingly promising candidate for major mobilization in U.S. healthcare data storage.⁹⁴ Instances of data privacy breaches, incomplete or inadequate privacy laws, and the commercialization of data have created the need for improved security and individualized user control. Blockchain, dependent upon these structures for its usage, represents a technology that independent health data storage could be built around.

The healthcare field is already implementing blockchain in the international market and sensitive PHRs offer a prime target for generating

Frameworks, in 11 IEEE ACCESS, 70110-12 (2023) (explaining that Blockchain, above alternative technologies, is useful for a building a secure transaction portal that is crucial for data governance).

⁸⁸ James Clavin et al., *Blockchains for Government: Use Cases and Challenges*, in DIGIT. GOV. RES. PRAC. 1, 3, (2020).

⁸⁹ Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 160, 162 (2011).

⁹⁰ Nathan Crooks, *What are blocks in a blockchain?*, THE BLOCK (Aug. 28, 2023), <https://www.theblock.co/learn/245697/what-are-blocks-in-a-blockchain>.

⁹¹ *Id.*

⁹² *Id.*

⁹³ Konstantinos Christidis & Michael Devetsikiotis, *Blockchains and Smart Contracts for the Internet of Things*, IEEE ACCESS (2016), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408>.

⁹⁴ Felix, *supra* note 39.

personalized data storage.⁹⁵ Individuals reliant on medical records for their safety and security can utilize existing technology to maintain records in a single location like a data wallet.⁹⁶ This wallet could provide user-specific information akin to a bank account while enabling the user to share certain aspects of their health records with chosen parties.⁹⁷ In practice, users could provide preset, approved data to an app they are interacting with, limiting an overflow of information they may not feel comfortable sharing. They could access a chronological chain of transactions about their personal health history, and share that information, without needing to go through a medical office's records department.

While enhancing user control, this blockchain approach maintains appropriate balance with legitimate public interests. The system does not create impenetrable walls around user data when legal access is warranted. Rather, it establishes a more transparent process where law enforcement can, with proper authorization such as a warrant, access an individual's ledger to verify transactions, frequency, and location.⁹⁸ The key difference lies in the heightened user awareness and control. Individuals with their PHRs more readily available to them could have greater understanding of what information exists about them and what specifically is being accessed, shifting from passive subjects of data collection to active managers of their personal health information.

A. Blockchain and Bitcoin

Separating the public's understanding of blockchain from cryptocurrency may be necessary for expanded use of blockchain in other industries. However, evidence suggests that blockchain is alive and well in industries separate of its financial inception and already solidifying its role within the healthcare field.⁹⁹ Its existing application in finance provides a foundation for buy-in from a heavily commercialized U.S. market, a task that can be difficult to achieve when navigating between industries. The popularity of the technology means that incentive exists for new models to be created, meeting the needs of the individual who desires more sovereign control over their personal health.¹⁰⁰

⁹⁵ See generally Huma Saeed et al., *Blockchain technology in healthcare: A systematic review*, PLOS ONE. (2022), <https://pmc.ncbi.nlm.nih.gov/articles/PMC9000089/>.

⁹⁶ Artoressi, *supra* note 24.

⁹⁷ *Id.*

⁹⁸ See Jason Weinstein, *How can law enforcement leverage the blockchain in investigations?*, COIN CTR. (Mar. 12, 2015), <https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/>.

⁹⁹ José Morey, *The Future of Blockchain in Healthcare*, FORBES (Oct. 25, 2021), <https://www.forbes.com/councils/forbestechcouncil/2021/10/25/the-future-of-blockchain-in-healthcare/>.

¹⁰⁰ Escobar, *supra* note 43.

Satoshi Nakamoto, the founder of Bitcoin, noted that the purpose of the blockchain model is to “completely decentralize” transactions.¹⁰¹ In his words, this method “eliminates the need for a questionable intermediary, such as a bank that piles fees on top of users,” and replaces it with a direct transaction portal that relies on individual user verification rather than needless checkpoints along the way.¹⁰²

While medical records may not be exactly one-to-one with banking or financing, the industries are connected and reliant on one another for success. Much like a financial transaction, accumulating medical records prior to a procedure involves accessing multiple “silos” of data.¹⁰³ These silos may appear as long-term health records, notes from a hospital stay, or even a ledger of pharmaceutical visits. By decreasing the trips to individual silos and enabling a user shareable access to their record, efficiency can be increased while “waste” is eliminated.¹⁰⁴

B. Cryptography

The peer-to-peer model that blockchain operates on is reliant on two security-based substructures: cryptography and hashing.¹⁰⁵

Cryptography is a method of securing data-based transactions, such as record of a medical visit in this instance, in such a way that an individual’s identity is not immediately distinguishable from others, yet their transaction is verifiable.¹⁰⁶ By providing pseudo-anonymity to a user, cryptography verifies a user’s identity without disseminating sensitive information about the business being conducted.¹⁰⁷ A user, as the owner of their information, can ensure only they or their verified users can access the details of a transaction.¹⁰⁸

A proper comparison can be made with an email account. A user may provide or make their email address publicly known, but added credentials provide the user with the ability to access their account and check their

¹⁰¹ See Maria Bustillos, *Annals of Technology: The Bitcoin Boom*, NEW YORKER (Apr. 1, 2013), <https://www.newyorker.com/tech/annals-of-technology/the-bitcoin-boom>.

¹⁰² *Id.*

¹⁰³ See generally *Blockchain: The Chain of Trust & Its Potential to Transform Healthcare—Our Point of View*, IBM (Aug 8, 2016), https://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf.

¹⁰⁴ See generally *id.*

¹⁰⁵ See Mark A. Engelhardt, *Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector*, TECH. INNOVATION MGMT. REV. (Oct. 2017), <https://www.timreview.ca/article/1111>.

¹⁰⁶ *Id.*

¹⁰⁷ See Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN, 19 (July 25, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

¹⁰⁸ *Id.*

inbox. While the user's identity can be managed for verification purposes, no business on the user's account can be accessed without adequate permission. Of course, email accounts get hacked, and users must still utilize reasonable care to ensure the security of their accounts. In practice, a method of storing vital medical information could be maintained at the user level while doctors, law enforcement, or other agencies are provided higher access by law, regulation, or user permission.

C. Hashes

Second, hashes, often referred to as digital fingerprints, represent a small bit of code or numerical data representative of a digital asset or transaction.¹⁰⁹ Hashing functions designed with cryptographic security in mind have developed as a way of promoting data integrity and digital authentication by reformatting each time even a minute change is made to an asset.¹¹⁰ When a user generates a hash by participating in a transaction, as defined by the parameters of the transaction, they create a hash that can be stored in a "block." Each subsequent transaction creates a new block that is chained to the previous data.¹¹¹ This chain of chronological transactions, a digital ledger, forms part of the underlying technology that makes blockchain valuable.

By generating multiple blocks in a chain, a user creates a verifiable chain of transactions over which they have primary authority.¹¹² At a high level, individual blocks, though connected, may only transmit data of a certain kind. Alternatively, these blocks could be designated to redact specific portions of a user's data in the event they are accessed by someone with inadequate permissions. Hashes serve the purpose of verifying that a transaction involving a specific user occurred, without alteration; however, they do provide more information than what is required for a specific function.¹¹³

D. Immutability

Blockchain sets itself apart from traditional forms of financial transactions with two primary forms of security-related data management: immutability and decentralization.

¹⁰⁹ Lianhua Chi & Xingquan Zhu, *Hashing Techniques: A Survey and Technology*, ACM COMPUTING SURV. vol. 50, Art. 11, 11-11:1 (2017), <https://www.cse.fau.edu/~xqzhu/papers/ACS.Chi.2017.Hashing.pdf>.

¹¹⁰ *Id.*

¹¹¹ Wright & De Filippi, *supra* note 107.

¹¹² *Id.*

¹¹³ Chi & Zhu, *supra* note 109.

Blockchain's immutability provides a portion of the technology's legitimacy that would benefit the health market, proof of work.¹¹⁴ Immutability means that once data is written to the blockchain, it cannot be altered or deleted without disrupting the entire chain of information.¹¹⁵ First, the inability of a chain to be altered, duplicated, or easily forged is a staple of the tamper proof technology and is present across most pioneering blockchains.¹¹⁶ As a technology designed to combat waste and eliminate instances of fraud, the inability for bad actors to change, delete, or replicate transactions produces a *trustless* system, devoid of reliance on third parties.¹¹⁷ While third parties may not be immediately necessary within the transaction, avenues become available for third parties to monitor instances of fraud, location-based inconsistencies, or an individual outright lying in their medical history.¹¹⁸

A final notable comment in the privacy-natured aspect of blockchain immutability is the experimental use of "permissioned" chains that enable a group of users to operate on a closed net.¹¹⁹ This technology would enable individuals to operate on a single chain, perhaps one day making a shared family medical record possible.¹²⁰ This technology is relatively new but may prove influential if blockchain continues to become more popular.

E. Decentralization

Blockchain fundamentally transforms data ownership using decentralized architecture. While the technology has certainly grown in popularity in recent years, it has always allowed for the decentralization and transparent, algorithmic verification of specific data.¹²¹ In Nakamoto's own vision for the open sale of Bitcoin, he references a desire to remove a single,

¹¹⁴ See Cornelius Agbo et al., *Blockchain Technology in Healthcare: A Systematic Review*, Healthcare (Basel), (Apr 4, 2019), <https://www.mdpi.com/2227-9032/7/2/56> (Blockchain's property of decentralization, immutability, data provenance, reliability, robustness, the smart contracts, security, and privacy, are being canvassed as the features that make it very suitable for storage and management of patients' electronic medical records (EMR).).

¹¹⁵ See Krisha Aranha, *What is Blockchain Immutability? – A Secure Tamper Proof Database*, MANGORESEARCH (May 21, 2018), <https://www.mangoresearch.co/blockchain-immutability/>.

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ Wright, *supra* note 107.

¹¹⁹ See Peng Zhang, *FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data*, COMPUT. STRUCTURE BIOTECHNOL. J. (July 29, 2019), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6082774/> (noting this platform, a so-called "permissioned" blockchain, is only accessible by authorized users who can then manage authentication, data sharing, and other security properties in the medical domain).

¹²⁰ *Id.*

¹²¹ Vikas Prajapati, *Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability*, 10 INT'L J. INNOVATIVE SCI. & RSCH. TECH., 1011-12 (2025), <https://doi.org/10.38124/ijisrt/25mar1062>.

governing entity from the transactional process.¹²² This, in theory, provides individuals with a level of sovereignty over their transactions not found in many processes, primarily because it eliminates a reliance on middlemen or intermediaries.¹²³ In the healthcare context, three advantages emerge.

First, individuals will have greater *autonomy* over their health data, a condition that can be limited due to the manner in which records are currently maintained. By granting individuals greater control over their PHRs, including the ability to access, manage, and share their records, their understanding of their own conditions is naturally enhanced.¹²⁴ This empowerment could foster a deeper knowledge of their health, enabling individuals to make more informed decisions. As a result, individuals can more effectively interact with applications utilizing their data, improving understanding of how their information may be being used.

Second, individuals will benefit from *disintermediation*, the removal of unnecessary or redundant trips to data silos that often contain a bulk of the same information with minute, nuanced differences.¹²⁵ With the shift to a system where PHRs are securely managed by the individuals themselves, there will be less need for healthcare providers to maintain records on-site, eliminating storage costs for businesses and reducing the transaction fee for users. This model could streamline the overall record management system by lowering both personal and institutional costs.

By empowering individuals to own and manage their health data, blockchain technology is poised to revolutionize the way PHRs are accessed and controlled. Next, section IV of this Note will discuss the necessary framework for this to succeed and the challenges ahead.

IV. REDEFINING PERSONAL HEATH: BLOCKCHAIN AND CONSUMER CONTROLLED RECORDS

A transition to blockchain for enhanced personal record-keeping would not be without challenges. To effectively harness this technology, users would first need to understand the blockchain basics that have been previously outlined.¹²⁶ Without proper understanding or training, blockchain users, including technology stakeholders, could end up more

¹²² See Bustillos, *supra* note 102.

¹²³ Prajapati, *supra* note 121, at 1014.

¹²⁴ *Id.*

¹²⁵ *Id.* at 1013.

¹²⁶ See *Blockchain: The Chain of Trust & Its Potential to Transform Healthcare--Our Point of View*, IBM (Aug 8, 2016), https://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf (challenges include technological know-how, storage limits, and accessibility with corporate legacy systems).

frustrated with than satisfied with new forms of record management.¹²⁷ As a technology proposed for the benefit of privacy and security, especially pertaining to sensitive personal health records, a lapse in understanding could only exacerbate how much data is in unwanted places.

Despite its transformative potential, Blockchain is not a universal solution, and, in many aspects, it is still in a testing phase.¹²⁸ As with any new technology, blockchain adoption is likely to face obstacles. User errors, problems with troubleshooting, regulatory lag, and scalability present challenges for deployers that will impact consumers as well.¹²⁹ Yet, despite these challenges, progress made in Blockchain research should refine these issues, making the technology more viable for widespread use. If properly implemented, the benefits of increased consumer protection outweigh the growing pains caused by implementation.

To succeed in the commercial market, developed blockchain technology would need to interface with current apps in a manner that is useful to users while maintaining robust privacy protections.¹³⁰ Apps that already harvest pharmacy records, routine care, health and exercise data, and other sensitive PHRs will require the ability to receive users' newly vetted information, ideally notifying users if what they have made available is or is not compatible with the app's functionality. Recognition of this data will likely require revisions to privacy policies, addressing a balance between what users make available and what data an app needs to properly function. The benefit of consumer-driven PHR management may appear in the form of informed consent. Individuals who are more informed about their data and what it is they are sharing can provide a more ascertainable form of consent.

Many companies possess the technology to support updated data integration, though the quality of these implementations vary.¹³¹ Moreover, with numerous consumer protection laws being implemented in the United States, companies are on notice that their client-based interactions may be changing. Some jurisdictions are already taking action—the state of Washington's "My Health, My Data Act" represents an early legislative attempt to regulate health data privacy and consumer control.¹³² This trend toward greater regulatory oversight creates both an opportunity and an urgency for blockchain implementation. By addressing technical and regulatory challenges through thoughtful planning, education, and

¹²⁷ Abu Naser Mohammad Saif et al., *Blockchain Implementation Challenges in Developing Countries: An Evidence-Based Systematic Review and Bibliometric Analysis*, TECH. INNOVATION MGMT. REV. (May 2022), <https://www.timreview.ca/article/1479>.

¹²⁸ Bojana Koteska et al., *Blockchain Implementation Quality Challenges: A Literature Review*, SEMANTIC SCHOLAR 8:4 (2017), paper-kot.pdf.

¹²⁹ *Id.*

¹³⁰ See Anderson, *supra* note 7.

¹³¹ *Id.* at 71.

¹³² See WASH. REV. CODE § 19.373 (2023).

collaboration with app developers, blockchain can become a cornerstone of consumer-controlled health data management. The following section will explore how these frameworks can effectively ensure blockchain's success.

A. Recoding Reproductive Rights: User-Focused Operation Challenges

While it is unlikely that abortion-related legislation is going to become easier to navigate, it is certain that the current Supreme Court believes the decision to codify abortion lies with the legislature and their constituents – a concept articulated by the majority in *Dobbs*.¹³³ For the time being, most consumers will operate under the data protection laws, much like the abortion laws, afforded them by their state. Providing individuals with a more secure process for controlling whom their data is shared with presents an opportunity to enable users to dictate how third parties access, store, and transfer their personal health information.

Implementation of such security measures, however, requires addressing significant regulatory challenges. Corporations that utilize individuals' data will need to be regulated to ensure they do so consistently with the proposed benefits of blockchain technology. Specifically, users should be provided the opportunity to provide information to data-driven companies that allows them to interface with a company's product without disseminating collateral personal information. Given notable lapses of individual privacy within the modern market, regulations that prevent data processors from collecting unnecessary user data should be put in place regardless of the speed in which blockchain can be implemented.¹³⁴ Several state privacy laws have been passed or slated for further discussion in upcoming legislative sessions that would require a company processing consumer data to maintain a written record of the data they are collecting, how it is to be stored, and for how long.¹³⁵

Colorado's Privacy Act provides a model for better defining categories of consumers. Specifically, it defines consumers as individuals who interface with technology as a part of their daily routine or home life.¹³⁶ These individuals are not expected to know the intricacies of data collection, storage, or production, and need not earn a technical degree to provide their consent.¹³⁷ Colorado's legislation places the burden to inform the consumer

¹³³ *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 302 (2022).

¹³⁴ See Matt Egan & Sam Lyngaas, *Nearly All AT&T Cell Customers' Call and Text Records Exposed in a Massive Breach*, CNN (July 12, 2024), <https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html>.

¹³⁵ See *Which States Have Consumer Data Privacy Laws?* BL (Mar. 18, 2024), <https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/>.

¹³⁶ COLO. REV. STAT. §§ 6-1-1303 (6) (2021).

¹³⁷ *Id.*

on the corporation or business who are expected to be well-versed in their business transactions and trained on the necessary regulation.¹³⁸ Bundles of laws like the ones seen in Colorado are rapidly emerging, shifting the regulatory playing field and requiring businesses to study the nuances that may exist from state to state.¹³⁹

B. Regulation Should Not Stifle Innovation

Regulators and law enforcement can find fruitful outcomes in a transition to a user-focused blockchain healthcare model. While documented ownership and trusted access to medical and administrative data is recognized as critical, the current processes need significant simplification and cost reduction to remain effective.¹⁴⁰ By enabling individuals more direct access to their PHRs, regulatory agencies can reposition to ensure that companies brokering data using sensitive consumer information in an ethical manner that contributes to consumer security and privacy. This approach mirrors blockchain's founding philosophy, which Satoshi Nakamoto described as removing "the need to trust a third party, or middleman" by replacing institutional intermediaries with systems based on proof instead of trust.¹⁴¹

In the same manner, law enforcement plays a significant role in maintaining trust in a digital world. Individual users with increased access to their PHRs arguably run a higher risk of exposure to fraudulent activity, a rapidly expanding market for threat actors.¹⁴² A properly supported transition towards a populace that is more knowledgeable about their online or app-based privacy rights is not something to be feared.

As reproductive health access becomes increasingly complex, well-defined expectations for how privacy should be regulated are critical for ethical enforcement. Traditional privacy frameworks like HIPAA, designed for conventional healthcare settings, are not helping the modern consumer or enforcer whose interests are locked to a phone screen. By reevaluating how data is stored or trafficked, modern legislation can eliminate vague

¹³⁸ Colo. Att'y Gen., Colorado Privacy Act, <https://coag.gov/resources/colorado-privacy-act/> (last visited Nov. 21, 2024).

¹³⁹ See *US State Privacy Legislation Tracker 2025*, IAPP, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (last visited Apr. 29, 2025).

¹⁴⁰ *Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View 3*, IBM (Aug. 8, 2016), https://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf.

¹⁴¹ See Bustillos, *supra* note 102.

¹⁴² See generally Emily Bonnie, *101 Data Privacy Statistics: The Facts You Need To Know In 2024*, SECUREFRAME (Mar. 5, 2024), <https://secureframe.com/blog/data-privacy-statistics>.

statutory interpretations and inconsistencies. This development, driven by the benefit to consumers, would likely prove useful in educating regulators, limiting arbitrary or unpredictable actions.

V. CONCLUSION

As reproductive healthcare access becomes increasingly digitized, the need for patient-controlled health data management is more present than ever. The legal landscape of healthcare is changing but the current legislation surrounding the rights of individuals and their interactions with data processors has not adapted alongside it. The intersection of technology, privacy, and reproductive rights presents a complex challenge. Blockchain technology offers a promising path to addressing interconnected issues, but without a larger regulatory framework for support, this may not get the lift needed to see the technology become successful. However, if meaningful trials occur that enable regulators and consumers to understand the potential of personalized health record management, then perhaps individuals can take greater control of their personal health records, potentially benefiting the consumer market as a whole.

The implementation of such a system is not without its hurdles. Technical complexities, the need for widespread adoption, and the challenge of regulating a commercial data market all present significant obstacles. However, the benefits of enhanced privacy, improved data security, and a safer approach to reproductive rights, make these challenges worth confronting.

Moving forward, lawmakers, technologists, and healthcare providers must work collaboratively on developing and implementing blockchain solutions that respect individual privacy while adhering to, at times, varying state laws. This approach can help mitigate the risks associated with current data management practices, reduce the potential for frivolous legal claims, and provide a more secure environment for sensitive health information.

The goal is to create a system that balances competing interests: respecting an individual's privacy rights, facilitating data processors need for accurate information, and accommodating legitimate legal requirements across jurisdictions. The current tension between privacy protection and regulatory compliance creates unnecessary vulnerability for all stakeholders. By embracing blockchain technology, we have an opportunity not just to enhance data security, but to fundamentally transform how we discuss personal health options and the ways in which we research and achieve them. The future for abortion rights is anything but certain but ensuring women can legally operate apps dedicated to their wellbeing without a fear for their safety is necessary in an era where digital privacy has never been more precarious or precious.