

HEALTH, PRIVACY, AND PRIVILEGE IN THE DIGITAL AGE

*Jonathan F. Will**

INTRODUCTION	965
I. MHEALTH APPS, DATA MARKETS, AND PRIVACY	
RISKS	970
II. DECISIONAL VERSUS INFORMATIONAL PRIVACY	980
III. PRIVILEGED COMMUNICATION WITH MHEALTH	
APPS	986
CONCLUSION.....	994

INTRODUCTION

The use of electronic, mobile health applications (“mHealth apps”) has become ubiquitous as individuals laudably take a more active role in their wellbeing. Such apps can be used for “health prediction, diagnosis, healthcare delivery, treatment support, chronic disease management,” and much more.¹ The astronomical growth in the amount of information shared with these apps has seen a corresponding explosion in the market for such data, all at a time when there are significant gaps in data protection due to the sectoral nature of privacy regulation in the United States.² An

*Director, Bioethics & Health Law Center, J. Will Young Professor of Law, Mississippi College School of Law. My thanks to the editorial staff of the *Mississippi Law Journal* for the invitation to participate in their symposium. This Article is based on my remarks at the symposium and the engaging discussion with fellow panelists attorney Melody McAnally, and Judges Michael Mills and David McCarty. Any errors are my own.

¹ Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 161 (2019).

² See generally Melody McAnally & Jennifer A. Svilar, *U.S. Privacy Law: Past, Present and Future*, PRO TE: SOLUTIO (Sep. 16, 2021),

individual's interest in keeping sensitive information private may clash with broader societal benefits that might be achieved by data sharing.³ While the market for data is staggering,⁴ access to information is not solely an economic enterprise. Interest groups and law enforcement also seek to obtain the information individuals upload into their various apps. These tensions come into stark focus in the context of reproductive health.⁵

Imagine the following scenario:⁶ a student⁷ suffering from debilitating cramps associated with menstruation attends a law school in the deep south.⁸ At a gynecologist appointment, the doctor asks several specific, intimate questions about the student's menstrual cycle, sexual activity, and cramp severity to gain as much information as possible—but the student admits to not keeping close track each month. The doctor recommends that the student utilize a cycle-tracking app (“CTA”) like Flo, which was the most widely downloaded CTA in the world as of November 2025.⁹

<https://protesolutio.com/2021/09/16/u-s-privacy-law-past-present-and-future/> [https://perma.cc/697A-7M75] (discussing the sectoral nature of privacy protection in the United States and the lack of a comprehensive data protection law).

³ Alan McQuinn, *The Economics of “Opt-Out” Versus “Opt-In” Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), <https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/> [https://perma.cc/KR9P-X3L4].

⁴ Revenue from internet advertising reached nearly \$260B in 2024. IAB & PWC, *INTERNET ADVERTISING REVENUE REPORT: FULL-YEAR 2024 RESULTS* 4 (2025).

⁵ Concerns regarding investigation and prosecution of pregnant people and health care providers are heightened since the Court overturned *Roe v. Wade*, 410 U.S. 113 (1973), overruled by *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022), but the types of digital surveillance described in this paper predate *Dobbs*. ALBERT FOX CAHN & ELENI MANIS, *PREGNANCY PANOPTICON: ABORTION SURVEILLANCE AFTER ROE* 1 (2022).

⁶ Law students made up a large portion of the symposium audience, so this paradigm case was meant to be provocative. The details are fictional, but not far-fetched. *See id.*; *see also infra* Part I.

⁷ Gender neutral language is used throughout this Article to acknowledge that menstruation and pregnancy are not limited to cis women. *See* KATE CLANCY, *PERIOD: THE REAL STORY OF MENSTRUATION* 15 (2023).

⁸ It is more typical of southern states to have abortion-restrictive legislation in the wake of the Supreme Court's *Dobbs* decision. *Interactive Map: US Abortion Policies and Access After Roe*, GUTTMACHER INSTIT. (Jan. 30, 2026), <https://states.guttmacher.org/policies/> [https://perma.cc/QV8E-6SM9].

⁹ Christy Tila, *Most Popular Period Tracking Apps 2025, by Downloads*, STATISTA (Nov. 28, 2025), <https://www.statista.com/statistics/1307702/top-period-tracker-apps->

Upon downloading the app, the student goes through the typical startup messages and prompts, quickly scrolling to the bottom and clicking “accept.” In a matter of moments, the app is up and running, offering numerous functions whereby the student can input the severity and duration of their cramps each month. The app can even make predictions about fertility windows that could, in theory, help as a form of birth control if the student also includes information about sexual activity and the use of contraception.¹⁰ Certain apps use data regarding basal body temperature (taken first thing in the morning) and cervical mucous to predict the timing of ovulation.¹¹ Unsurprisingly, the more accurate the data inputted, the more accurate the results.

Impressed with the functionality, the student dutifully inputs data every month. As the stress of finals approaches, the student thinks nothing of recording the fact that the student did not have a period in December.¹² As an after-finals reward, the student travels to New York City¹³ for a long weekend, and by the time classes restarted in January, the student’s cycle is back on track with life, continuing in unremarkable fashion.

At least for a brief time, because behind the scenes there was additional activity. Part of what the student consented to when setting up the app was the compilation and sale of the data entered. On an individual basis, a person’s information is not

worldwide-by-downloads/ [https://perma.cc/K6QL-TFKS] (identifying London-based *Flo* as the most globally downloaded period tracking as of November 2025). The top three CTAs exceeded 250 million downloads in 2024. STEFANIE FELSBERGER, *THE HIGH STAKES OF TRACKING MENSTRUATION* 9 (2025).

¹⁰ Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. 1233, 1253-55 (2023).

¹¹ *Id.*

¹² See Swapna Kollikonda, *How Stress Can Impact Your Menstrual Cycle*, CLEV. CLINIC: HEALTH ESSENTIALS (Sep. 24, 2025), https://health.clevelandclinic.org/can-stress-cause-you-to-skip-a-period [https://perma.cc/P946-HVPJ] (explaining that elevated levels of cortisol caused by stress can lead to delayed, light, or completely missed periods).

¹³ In the aftermath of *Dobbs*, New York passed abortion protective shield laws protecting providers and pregnant persons. See S.B. S1066B, 2023 Gen. Assemb., Reg. Sess. (N.Y. 2023) (codified as amended in various sections of N.Y. law) (amending criminal procedure law, civil practice law and rules, insurance law, and education law to protect abortion providers and patients from out-of-state investigations); see also GUTTMACHER INST., *supra* note 8.

particularly valuable,¹⁴ but when aggregated, the data joins a digital marketing economy worth billions of dollars per year.

The compiled data is also of interest to law enforcement, which can acquire the data without a warrant pursuant to the third-party doctrine and run its own machine learning algorithms to identify suspicious activity.¹⁵ In the context of the law student, for instance, artificial intelligence (“AI”) could evaluate innumerable data points to flag individuals who missed their periods coinciding with sexual activity. From there, geolocation data can be cross-referenced to identify a subset of persons who traveled from abortion-restrictive jurisdictions to those with more permissive laws, and whose cycles restarted within a sixty-day window. Such information could then be used to secure a warrant, which the law student would learn when police arrived to confiscate their electronic devices.

This scenario is not a prediction of a distant dystopian world ripped from the pages of Huxley or Orwell.¹⁶ The technology described already exists and is being used.¹⁷ The paradigm is similarly not intended as commentary on the morality of abortion. It is about the accessibility and use of a person’s intimate health information; data the person may have assumed would be entitled to privacy protection, only to find that it often is not. While the permissibility of abortion may be hopelessly intractable, polls indicate that there is bipartisan support for protecting privacy as

¹⁴ McQuinn, *supra* note 3 (noting that when purchased in bulk, each individual user’s data is worth roughly \$0.005).

¹⁵ See *infra* Part I. Machine learning allows a given system to learn from experience and make adjustments itself without the need for specific programming. Such algorithms are a type of artificial intelligence that process real-world data to identify and learn patterns about individual and business behaviors and transactions. See Iqbal H. Sarker, Machine Learning: Algorithms, Real-World Applications and Research Directions, 2 SN COMPUT. SCI. 160, 161-63 (2021).

¹⁶ See *generally* ALDOUS HUXLEY, BRAVE NEW WORLD (Harper & Bros. 1932); GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Secker & Warburg 1949) (each describing a future with increased government surveillance and restrictions on reproduction).

¹⁷ See, e.g., CAHN & MANIS, *supra* note 5, at 3-6; Cynthia Conti-Cook & Kate Bertash, *Digital Surveillance Presents New Threats to Reproductive Freedoms*, WASH. POST (Dec. 15, 2021), <https://www.washingtonpost.com/outlook/2021/12/15/digital-surveillance-reproductive-freedom/> [<https://perma.cc/UP6J-SM93>] (detailing instances of digital surveillance used in police investigations).

a general matter,¹⁸ and the Constitution itself constrains investigatory practices.¹⁹ After all, just as humans are susceptible to implicit bias, so too are the data generated by such humans and the algorithms created to process that data.²⁰

Part I of this Article provides an overview of the growth of mHealth apps (and of CTAs in particular) as individuals take a more active role in managing their health. The market for this intimate health information at a time when privacy protection is limited creates significant concerns. This section draws attention to the narrow reach of the Health Insurance Portability and Accountability Act (“HIPAA”) and introduces the third-party doctrine in the context of warrantless access to information in criminal investigations. Data producers often misunderstand the extent to which their information is protected, which makes inadvertent disclosure to advertisers, law enforcement, and interest groups a problem.

In search of greater protection, Part II explores the nature of an informational privacy right first referenced in *Whalen v. Roe*²¹ as distinct from the substantive due process privacy right that once protected the decision to terminate a pregnancy.²² Even as the Court’s *Dobbs* decision overturned *Roe v. Wade*, Justice Alito’s majority opinion highlighted this privacy distinction.²³ While the Supreme Court and lower courts have consistently indicated that individuals expect that their health information will be private, the scope of any constitutionally protected right of informational privacy remains elusive, and, as such, overreliance on informational privacy to fill in privacy gaps proves unsatisfying.

While other scholars have provided suggestions for how greater protection might be realized (such as increased individual

¹⁸ See, e.g., *Public Opinion on Privacy*, ELEC. PRIV. INFO. CTR., <https://archive.epic.org/privacy/survey/> [<https://perma.cc/RQZ6-MMZ7>] (last visited Feb. 21, 2026) (indicating that 86% of Democrats and 81% of Republicans support a federal privacy bill).

¹⁹ U.S. CONST. amend. IV.

²⁰ Lorenzo Belenguer, *AI Bias: Exploring Discriminatory Algorithmic Decision-Making Models and the Application of Possible Machine-Centric Solutions Adapted from the Pharmaceutical Industry*, 2 AI & ETHICS, 771, 773 (2022).

²¹ 429 U.S. 589, 598-600 (1977).

²² *Roe v. Wade*, 410 U.S. 113, 153 (1973).

²³ *Dobbs v. Jackson Women’s Health Org.*, 597 U.S. 215, 273 (2022).

accountability, expansion of HIPAA, or more comprehensive data protection laws),²⁴ this Article offers a novel, if modest, approach. Given the difficulty in keeping digital information truly private, Part III argues that enhanced protection could be achieved through recognition of an evidentiary privilege that covers information shared with mHealth apps, including CTAs.²⁵ The privilege is an extension of the confidentiality necessary to ensure that patients honestly and accurately provide information to their physicians when seeking treatment and medical advice. Such open communication promotes the autonomous decision making of patients, and the same theories that offer normative justification for such protection apply with equal force as individuals more frequently interact with apps to achieve their health goals.

I. MHEALTH APPS, DATA MARKETS, AND PRIVACY RISKS

Individuals seeking to gain greater control over their wellbeing commonly use mHealth apps and websites. As one scholar noted, the apps are used “in almost every area of medicine and health, including dermatology, maternal, newborn, and child health, and communicable and contagious diseases, just to name a few.”²⁶ A recent Kaiser poll found that 75% of participants used a health tracking app or website to manage their health within the past year.²⁷ While the two most commonly reported reasons for

²⁴ See, e.g., Fowler & Ulrich, *supra* note 10, at 1309-12; Stacey A. Tovino, *Aborted Confidentiality*, 65 B.C. L. REV. 1921, 1975-78 (2024). For other suggestions, see generally Travis Handler, Comment, *Byte by Byte: Breaking Down the Third-Party Doctrine and Reproductive Health Apps After Dobbs*, 77 OKLA. L. REV. 669 (2025); Carmel Shachar & Carleen Zubrzycki, *Informational Privacy After Dobbs*, 75 ALA. L. REV. 1 (2023).

²⁵ Others have suggested new privilege laws that specifically cover abortion-related information. See Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV. 555, 635-42 (2023); Tom Lininger, *Abortion, the Underground Railroad, and Evidentiary Privilege*, 80 WASH. & LEE L. REV. 663, 721-23 (2023). While such laws may pass in abortion permissive states, the protection of abortion-specific information would not likely be a viable option in abortion restrictive states. Focusing more generally on information shared with health maintenance apps may be more palatable.

²⁶ Tovino, *supra* note 1, at 161-62.

²⁷ See Grace Sparks et al., *KFF Health Tracking Poll: Public Use and Trust in Health Care Apps and Websites*, KFF (Oct. 24, 2025) <https://www.kff.org/public-opinion/kff-health-tracking-poll-public-use-and-trust-in-health-care-apps-and-websites/> [https://perma.cc/4V8H-EHC5]. The increasing use of self-surveillance technology is

using apps or websites were to access medical records/lab results (75%) or to manage prescriptions (62%), many users also communicated directly with a health care professional via technology (57%), and over 20% used an app or website to manage a chronic condition like diabetes or obesity.²⁸

Chronic, noncommunicable diseases such as cardiovascular disease, chronic respiratory disease, cancer, and diabetes “are the main cause of death and morbidity worldwide.”²⁹ There is hope that effective mHealth apps such as medical sensors, activity trackers, wearables, and even simple applications into which users input data, will lead to improved patient self-monitoring and medical diagnosis and treatment.³⁰ Indeed, the use of AI in conjunction with mHealth apps shows promise in terms of personalized health and healthcare delivery, disease monitoring and prevention, and decreased time and costs.³¹

The World Health Organization (“WHO”) recognizes that digital health interventions can be used to address health system challenges such as low demand for services, poor adherence to guidelines, and access issues associated with geography and insufficient supply of healthcare products and service providers.³² At the same time, the WHO acknowledges quality and privacy concerns associated with the use of digital devices given that, by definition, intimate health information is being collected and transmitted.³³

In the United States, a given mHealth app or digital intervention may be considered a medical device, but the level of regulation imposed by the Food and Drug Administration (“FDA”)

nothing new. *See generally* Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809 (2012) (discussing the rise of technology, the already common concerns raised about privacy, and suggesting a new “data guardian” concept to offer more protection).

²⁸ Sparks et al., *supra* note 27.

²⁹ Alejandro Deniz-Garcia et al., *Quality, Usability, and Effectiveness of mHealth Apps and the Role of Artificial Intelligence: Current Scenario and Challenges*, 25 J. MED. INTERNET RSCH. 44030 (2023), <https://www.jmir.org/2023/1/e44030> [<https://perma.cc/ZBY9-MNZ6>].

³⁰ *Id.*

³¹ *Id.*

³² WORLD HEALTH ORG., WHO GUIDELINE RECOMMENDATIONS ON DIGITAL INTERVENTIONS FOR HEALTH SYSTEM STRENGTHENING 5-6 (2019).

³³ *See, e.g., id.* at 11, 37, 42, 49.

is tied to risk.³⁴ Broadly speaking, the FDA has acknowledged the importance of using technology “to motivate a person to stay healthy,” and therefore takes a “very light touch, an almost hands off approach”³⁵ to monitoring the industry. The administration “generally does not regulate medical apps, limiting its review of medical devices to those that pose patient safety risks in the event of device failure.”³⁶ While fewer regulatory requirements may reduce the costs of developing and operating such apps, thus making them more accessible, the lack of oversight exposes users to risk. The relevant issues are amplified in the context of CTAs in particular.

Menstrual health is an under-researched area. The studies that exist primarily focus on reproduction, which leaves wide knowledge gaps associated with the ways in which menstruation impacts everyday life.³⁷ CTAs, in their various forms, help to bridge the divide by empowering individual users through “self tracking, data science, and AI.”³⁸ For instance, in addition to providing information on fertility windows, apps can track details about emotions, premenstrual syndrome, and bodily functions throughout the menstrual cycle.³⁹ For those with irregular periods, algorithms can assess numerous data points to provide predictions on future cycles.⁴⁰ In this sense, CTAs can be empowering for users,⁴¹ especially for those with conditions such as “poly-cystic ovary syndrome, endometriosis, or Premenstrual

³⁴ Fowler & Ulrich, *supra* note 10, at 1255 (discussing the classification scheme for medical devices and noting that apps indicating use as contraceptive devices are generally regulated by the FDA).

³⁵ Stephanie Baum, *FDA Assoc Director of Digital Health: We Are Taking Almost Hands-Off Approach*, MEDCITYNEWS (Mar. 31, 2015, at 09:00 CT), <https://medcitynews.com/2015/03/fda-assoc-director-digital-health-taking-almost-hands-approach/> [<https://perma.cc/9AKD-CNHX>].

³⁶ Michele Estrin Gilman, *Periods for Profit and the Rise of Menstrual Surveillance*, 41 COLUM. J. GENDER & L. 100, 110 (2021) (citing *Device Software Functions Including Mobile Medical Applications*, FDA (Nov. 5, 2019), <https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications> [<https://perma.cc/D2EV-FEP8>]).

³⁷ FELSBERGER, *supra* note 9, at 13.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.* at 14.

⁴¹ Fowler & Ulrich, *supra* note 10, at 1257-58.

Dysphoric Disorder, which can go undiagnosed for years.”⁴² What is more, CTAs are often downloadable for free, though fees may be associated with premium features.⁴³

It is not surprising that CTAs enjoy widespread popularity. As mentioned, the top three apps numbered 250 million downloads as of 2024.⁴⁴ Specific to the United States, a recent study found that use of CTAs increased from 37% to 45% after *Dobbs* was decided.⁴⁵ Each day, users dutifully upload intimate information about menstruation, sexual activity, cervical mucus, and more. In a short period of time, apps accumulate tremendous amounts of data—data that is extremely valuable. By 2020, the femtech market, which includes digital products, services, and technologies aimed at women’s health, reached \$20 billion. It is expected to exceed \$60 billion by 2027, and half of that market comes from CTAs.⁴⁶

Many of the apps are specifically designed with the intention to collect, aggregate, and sell data.⁴⁷ One estimate from 2014 found that in the broader market for personal information, a pregnant person’s data is worth fifteen times that of the average person because pregnant individuals “actively seek new products, develop new brand loyalties, and purchase in bulk during pregnancy and after birth.”⁴⁸ Given the lucrative nature of the industry, the privacy interests of users may not be of primary concern to profit-seeking app developers.⁴⁹

What is more, users frequently do not fully appreciate the extent to which the intimate information they upload is exposed. At times, users consent to the sale of their data by failing to read the terms and conditions to which they agree when using the app,

⁴² FELSBERGER, *supra* note 9, at 13.

⁴³ *Id.* at 15. Unsurprisingly, CTAs that are regulated by the FDA are not free. One such example, Natural Cycles, has a \$99.99 annual subscription plus an additional fee for a basal thermometer. Fowler & Ulrich, *supra* note 10, at 1275. These costs are not insignificant and may create socio-economic disparities in access. *Id.* at 1275.

⁴⁴ FELSBERGER, *supra* note 9, at 9.

⁴⁵ Rowena Lindsay, *Period Apps After Dobbs: More Users, More Risks*, PUB. HEALTH POST (Apr. 7, 2025), <https://publichealthpost.org/sexual-reproductive-health/period-apps-after-dobbs-more-users-more-risks/> [https://perma.cc/GP7K-P6CE].

⁴⁶ FELSBERGER, *supra* note 9, at 9.

⁴⁷ Fowler & Ulrich, *supra* note 10, at 1265.

⁴⁸ *Id.* at 1265-66.

⁴⁹ Gilman, *supra* note 36, at 102.

which is not shocking.⁵⁰ As Professor Gilman notes, “[n]umerous studies show that consumers do not, and cannot, read privacy policies that are lengthy and rife with legalese.”⁵¹ These types of clickwrap provisions are rightly challenged as not representing meaningful consent.⁵²

More troubling, there are increasing incidences of app developers that do not accurately describe their privacy policies or share data without any sort of consent. Professors Fowler and Ulrich note that “87% of sampled apps shared user data with third parties, though only 70% discussed data processing transparently, 26% did not discuss it at all, and 35% did not provide information about data security.”⁵³ For its part the Federal Trade Commission (“FTC”) settled a case against the CTA Flo (with over 100 million users) that alleged the app was sharing data with Facebook and Google, notwithstanding a promise to users that their data would remain private.⁵⁴ Similarly, the Attorney General of California settled a case against Glow, a CTA found to have allowed third-party access to user data without user consent.⁵⁵ While the FTC has authority to hold app developers accountable for unfair trade practices, the reach is limited given the absence of a comprehensive data protection law in the United States that would impose more stringent privacy obligations.⁵⁶

Beyond this, users of mHealth apps may not adequately anticipate the sale of their data because they incorrectly assume that HIPAA protects the private health information they are uploading.⁵⁷ The disconnect stems from the fact that HIPAA protection is tied to certain covered entities, not the type of data in question. HIPAA Rules only apply to “(1) health plans, healthcare

⁵⁰ Fowler & Ulrich, *supra* note 10, at 1269 (citing DELOITTE, 2017 GLOBAL MOBILE CONSUMER SURVEY: US EDITION: THE DAWN OF THE NEXT ERA IN MOBILE 12 (2017) (finding that over 90% of individuals surveyed consented to terms and conditions without reading them)).

⁵¹ Gilman, *supra* note 36, at 110.

⁵² See *infra* Part III (suggesting that inadvertent “consent” should not necessarily constitute a waiver of privilege protection).

⁵³ Fowler & Ulrich, *supra* note 10, at 1267.

⁵⁴ Gilman, *supra* note 36, at 103.

⁵⁵ *Id.* at 104.

⁵⁶ McAnally & Svilar, *supra* note 2.

⁵⁷ See, e.g., Leah R. Fowler, *COVID-19 & the Myth of Health Data Privacy*, 31 KAN. J.L. & PUB. POLY 373, 380-83 (2022); Tovino, *supra* note 1, at 176.

clearinghouses, and those healthcare providers that transmit health information in electronic form in connection with standard transactions, including health insurance claims [covered entities]; and (2) persons or entities that access or use protected health information to provide certain services to, or to perform certain functions on behalf of, covered entities [business associates].”⁵⁸ While data inputted into an app that is developed and utilized by a covered entity or business associate might be protected by HIPAA,⁵⁹ the law simply does not cover the massive amount of intimate health data shared with most mHealth apps.⁶⁰

Extending HIPAA to cover mHealth apps would require developers to obtain written authorization prior to sharing an individual’s protected health information.⁶¹ Until that time, HIPAA itself does not prevent the sale of user data, which makes it all the more important for users to be aware of the privacy policies (or lack thereof) implemented by the apps they utilize. Users concerned about their privacy should opt out of data sharing whenever possible and also store their information solely on their devices; that is, they should not allow the data to be stored on online platforms like the cloud.⁶² These efforts may not ultimately be adequate to ensure complete privacy, but they reflect an affirmative attempt to keep the information confidential.⁶³

In practice, the annoyance of unsolicited advertisements may not be a sufficient incentive for individuals to read small print terms and conditions. While people often speak of their interest in privacy, behavioral studies suggest that they are not inclined to pay for it.⁶⁴ In one experiment only eleven percent of participants

⁵⁸ Tovino, *supra* note 1, at 157-58.

⁵⁹ *Id.* at 174-75 (discussing application of HIPAA rules to covered entities).

⁶⁰ Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 425 (2018); Lininger, *supra* note 25, at 713. Scholars such as Andrews, Fowler, Gilman, Tovino, and Ulrich cited herein have persuasively argued that HIPAA ought to be expanded to include mHealth apps and CTAs. The purpose of this paper is to identify a different type of protection to be found through recognition of an evidentiary privilege that covers information shared with such mHealth apps or CTAs. See *infra* Part III.

⁶¹ Tovino, *supra* note 1, at 181-82.

⁶² Fowler & Ulrich, *supra* note 10, at 1311-12.

⁶³ See *infra* Part III. Maintaining the confidence of the information would be an important aspect of the privilege assessment.

⁶⁴ McQuinn, *supra* note 3.

were willing to pay a single dollar for data protection services, and another found that ninety percent preferred a \$12 gift card instead of a \$10 gift card that included data protection.⁶⁵

The studies are limited, but there is at least some evidence to suggest that people are concerned about privacy as long as it is free. This is important because the “free” nature of mHealth apps is obviously being subsidized by the backend monetization of the data collected.⁶⁶ If the market for such data decreases (due to folks opting out of data sharing or greater legal privacy protections being imposed), the cost of the apps will surely increase. But beyond the price of apps, users should also understand that the AI algorithms assessing the data are far from perfect, and it is not only advertisers interested in their information.

While early studies indicate that AI shows promise to increase diagnostic accuracy and has proven “effective as a support system for self-management” of certain diseases, challenges remain.⁶⁷ Perhaps ironically, AI capabilities are constrained by the quality and quantity of the data available, with greater access to information leading to more effective applications.⁶⁸ Therefore, the success of AI diagnostics and predictions are limited by the availability of the very information users may want to protect.

In the context of unregulated CTAs, there are serious concerns about the accuracy of predictions users receive, which could lead to unintended pregnancies.⁶⁹ In theory, one option to increase the available data without jeopardizing privacy is to de-identify the information at the outset. Unfortunately, it is well understood that health information, in particular, can often be re-identified given the highly personal nature of the information involved.⁷⁰ Again, ironically, the power of AI tools makes this re-identification process easier.

⁶⁵ *Id.*

⁶⁶ See Huq & Wexler, *supra* note 25, at 623 (“To be sure, electing not to share or sell certain data to brokers and other third parties will likely create economic costs for technology companies.”).

⁶⁷ Deniz-Garcia, *supra* note 29, at 16.

⁶⁸ *Id.*

⁶⁹ Fowler & Ulrich, *supra* note 10, at 1262-65; FELSBERGER, *supra* note 9, at 14.

⁷⁰ I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 JAMA 231, 231-32 (2018).

One of the greatest concerns associated with how AI assesses data is the risk of bias, which occurs when the AI output discriminates against specific groups or individuals.⁷¹ Bias arises “because of prejudiced assumptions in the process of developing the [AI] model, or non-representative, inaccurate or simply wrong training data.”⁷² In other words, bias can stem from faulty algorithmic design, or from embedded flaws in the data being assessed. Collectively, the risk is that AI modalities may “amplify human biases, replicate toxic language, or perpetuate stereotypes of gender, sexual orientation, political leaning, or religion.”⁷³

These issues are all the more troublesome given the ways in which CTA data is already being used because, again, the information is not just sought by advertisers. For instance, an anti-abortion interest group could conceivably develop an algorithm in an effort to scan available CTA data to target individuals from demographics statistically more likely to terminate a pregnancy.⁷⁴ Even prior to *Dobbs*, law enforcement used digital data to investigate persons suspected of self-inducing abortion,⁷⁵ and such data leveraging is only expected to increase in the years following.⁷⁶

This new digital-surveillance age is not limited to abortion. Law enforcement has used geofence warrants for years in various types of investigations,⁷⁷ and under third-party doctrine, police

⁷¹ Belenguer, *supra* note 20, at 773.

⁷² *Id.*

⁷³ Parker Brown, Comment, *Patient Records to Client Files: How the Legal Profession's Confidentiality Standards Can Inform Healthcare Corporations' Approach to Artificial Intelligence to Minimize HIPAA Violations*, 95 MISS. L.J. (forthcoming 2026) (citing Stefan Feuerriegel et al., *Generative AI*, 66 BUS. & INFO. SYS. ENG'G 111, 116 (2024)).

⁷⁴ See Fowler & Ulrich, *supra* note 10, 1237 n.14 (describing a Christian services group and network of crisis pregnancy centers that used geofencing and mobile data to disseminate targeted anti-abortion materials); Abigail Abrams & Vera Bergengruen, *Anti-Abortion Pregnancy Centers Are Collecting Troves of Data That Could Be Weaponized Against Women*, TIME (June 22, 2022, at 11:02 CT), <https://time.com/6189528/anti-abortion-pregnancy-centers-collect-data-investigation/> [<https://perma.cc/W9B9-6KVJ>].

⁷⁵ Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 50-51 (2020).

⁷⁶ See, e.g., Fowler & Ulrich, *supra* note 10, at 1237-38; Huq & Wexler, *supra* note 25, at 586; Lininger, *supra* note 25, at 695-96.

⁷⁷ Geofence warrants are used to identify cell phone users who were within a given distance of a location during a specified timeframe. Huq & Wexler, *supra* note 25, at

can often acquire information from data brokers without first obtaining a warrant.⁷⁸ Of relevance here, third-party doctrine is premised on the notion that if you voluntarily convey information to a third party, you no longer retain an expectation of privacy, which removes the Fourth Amendment as an investigatory hurdle.⁷⁹

The issue is plain. If users voluntarily convey their intimate health information to a mHealth app like a CTA, which then sells the data to a third party, arguably law enforcement could access such information without a warrant. The argument would be especially strong where the user affirmatively consents to such sale by accepting unread terms and conditions, which calls to mind the importance of user awareness of relevant privacy policies. That said, the Supreme Court's holding in *Carpenter v. United States*⁸⁰ may provide ammunition for a privacy protectionist position.

In *Carpenter* the Court determined that individuals retain an expectation of privacy in their cell-site location information ("CSLI") and, as such, this information cannot be obtained without a warrant.⁸¹ The Court reasoned that although users might consent to their cell phones tracking their location—for instance, to give directions or nearby restaurant recommendations—given the breadth of data then available about the individual via CSLI, such expansive information should not be considered voluntarily given.⁸² The ultimate reach of *Carpenter* remains to be seen, so it is unclear whether a user could be found to retain an expectation of privacy in health information voluntarily uploaded into an

577, 605 (highlighting that Google was served with nearly 6,000 geofence warrants between 2018 and 2020 in states that now have strict abortion restrictions since *Dobbs*).

⁷⁸ Handler, *supra* note 24, at 677.

⁷⁹ *Id.* (first citing *Smith v. Maryland*, 442 U.S. 735, 744-46 (1979); and then citing *United States v. Miller*, 425 U.S. 435, 443-44 (1976)).

⁸⁰ 585 U.S. 296, 316-17 (2018).

⁸¹ *Id.* at 310-16.

⁸² *Id.* at 314 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (alteration in original) (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979))).

mHealth app.⁸³ This issue is explored more fully in Part III when justifying the recognition of an evidentiary privilege protecting such information. The privilege would narrow the circumstances under which intimate health data could be accessed.

In the meantime, it is important to round out the aforementioned concerns by drawing attention to the fact that investigations do not equally impact all people. Even where privacy protections exist, there are exceptions for law enforcement purposes.⁸⁴ History has shown time and again that “police surveillance will fall more heavily on minority communities due to bias (both explicit and implicit), as well as the longstanding concentration of law enforcement resources in those areas and the shortfall of legal representation for people of color.”⁸⁵

When inferences and assumptions are involved, certain populations, namely women and minorities, often receive disparate treatment. They are more likely to be assumed to be engaged in illicit behavior, for instance, when a miscarriage occurs. For example, a review of the drug-testing policy challenged in *Ferguson v. City of Charleston*⁸⁶ found that only one of the dozens of women charged was white.⁸⁷ Recall that the AI algorithms being utilized will be constrained by these historical facts unless and until they are trained to avoid such bias.

Use of mHealth apps (including CTAs) and AI is ever increasing. The vast amounts of data that must be shared to effectively utilize these technologies create privacy risks for users at a time where we lack a comprehensive data protection framework in the United States. There are some affirmative steps individuals can take, but it is increasingly difficult to keep data truly private.

⁸³ There is an argument that misunderstanding the reach of HIPAA could actually be evidence of a retained expectation of privacy related to health data uploaded into apps. Handler, *supra* note 24, at 680; Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1097-98 (2023).

⁸⁴ Fowler & Ulrich, *supra* note 10, at 1299-300.

⁸⁵ Lininger, *supra* note 25, at 699.

⁸⁶ See generally *Ferguson v. City of Charleston*, 532 U.S. 67 (2001). See discussion of *Ferguson* *infra* Part II.

⁸⁷ Grace Howard, *The Pregnancy Police: Surveillance, Regulation, and Control*, 14 HARV. L. & POL'Y REV. 347, 352 (2020).

The reversal of *Roe v. Wade* sparked a flurry of articles regarding reproductive data privacy with students and established scholars writing dozens of papers.⁸⁸ Part of the tension is due to the fact that the ability to choose to terminate a pregnancy recognized in *Roe* was founded on a decisional privacy right rejected in *Dobbs*.⁸⁹

Part II now turns to the distinction between the Supreme Court's consideration of decisional privacy versus the informational privacy more directly at issue in cases involving access to data uploaded to mHealth apps.

II. DECISIONAL VERSUS INFORMATIONAL PRIVACY

Decisional privacy falls under the umbrella of substantive due process rights and thus has a fraught history. Regardless of one's views regarding the morality of abortion, because the word privacy does not appear in the text of the Fourteenth Amendment,⁹⁰ Justice Blackmun's opinion in *Roe* has been criticized from the outset.⁹¹ To be sure, issues surrounding decisional privacy and substantive due process are not limited to abortion.

While acknowledging substantive due process as a source of rights, Justice Rehnquist wrote more recently in the context of end-of-life decision-making that the Court must "exercise the utmost care" in this area because when recognizing such rights, the Court "place[s] the matter outside the arena of public debate and legislative action."⁹² Such expansion of rights, Rehnquist feared, would transform "the liberty protected by the Due Process Clause . . . into the policy preferences of the Members of this Court."⁹³

⁸⁸ A topic-specific Westlaw search returned dozens of articles published since 2023 alone.

⁸⁹ See *supra* notes 22-23 and accompanying text.

⁹⁰ U.S. CONST. amend. IV.

⁹¹ See generally John Hart Ely, *The Wages of Crying Wolf: A Comment on Roe v. Wade*, 82 YALE L.J. 920 (1973) (challenging the Court's reasoning not regarding the morality of abortion, but on the lack of textual foundation for the right established).

⁹² *Washington v. Glucksberg*, 521 U.S. 702, 720 (1997).

⁹³ *Id.* This language was also cited by Justice Alito in *Dobbs*. *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 240 (2022).

It is beyond the scope of this Article to resolve or even fully discuss the validity of unenumerated Constitutional rights, a topic that has been debated at least since the Federalist Papers at the country's founding. In Federalist No. 84, Alexander Hamilton wrote of his concern that creating a Bill of Rights might imply that unlisted rights are not protected,⁹⁴ which is problematic for those in favor of a government of limited powers.

For purposes here, it is sufficient to acknowledge that when governments pass laws that restrict fundamental rights, such laws are subject to strict scrutiny review and are unlikely to survive.⁹⁵ That was precisely Rehnquist's point about removing the matter from public debate and legislative action, and it is a conceptual challenge that exists with any matter suggested to be encompassed in a right of decisional privacy. In short, if a law that impacts one's ability to make any decision is subject to strict scrutiny, governments would have a difficult time passing laws indeed. The question of which decisions ought to be protected is where the proverbial rubber hits the road. And after *Dobbs*, the decision to terminate a pregnancy is no longer protected.

Even still, while Justice Thomas seemed open to revisiting (and likely reversing) all of the Court's prior decisions recognizing substantive due process rights,⁹⁶ Justice Alito's opinion did not go that far.⁹⁷ But more relevant for purposes here, Justice Alito also drew attention to a separate, informational privacy right that is distinct from any conception of decisional privacy. Specifically, Alito stated that "*Roe* conflated the right to shield information from disclosure and the right to make and implement important

⁹⁴ THE FEDERALIST NO. 84 (Alexander Hamilton).

⁹⁵ Strict scrutiny requires that the government have a compelling interest and that the law in question be narrowly tailored (or the least restrictive means) of furthering that interest. Professor Gunther famously (or infamously) referred to the test as strict in theory, fatal in fact. Gerald Gunther, *Foreword: In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972).

⁹⁶ *Dobbs*, 597 U.S. at 331-36 (Thomas, J. concurring).

⁹⁷ See *id.* at 262 (majority opinion) (calling "unfounded" the dissent's suggestion that the majority opinion endangers other substantive due process rights as well, such as those established in *Griswold v. Connecticut*, 381 U.S. 479 (1965) (contraception); *Eisenstadt v. Baird*, 405 U.S. 438, (1972) (contraception); *Lawrence v. Texas*, 539 U.S. 558 (2003) (same-sex sexual conduct); and *Obergefell v. Hodges*, 576 U.S. 644 (2015) (same-sex marriage)).

personal decisions without governmental interference.”⁹⁸ As discussed, *Roe*’s reliance on a decisional privacy right is what was overturned in *Dobbs*, but Alito’s citation to the Court’s opinion in *Whalen* at least implicitly signals approval of some sort of right to informational privacy.⁹⁹

In fact, *Dobbs* wasn’t the first time Justice Alito called upon *Whalen*. A decade before authoring the *Dobbs* decision, Alito wrote an opinion considering the permissibility of a background check protocol utilized by NASA that included disclosure of information associated with treatment or counseling for substance abuse.¹⁰⁰ The Court assumed, without deciding, “that the Constitution protects a privacy right of the sort mentioned in *Whalen*”¹⁰¹ (and a later case *Nixon*)¹⁰² but ultimately held that the government had a sufficiently reasonable interest in gathering the information.¹⁰³

The scope of any right to informational privacy is unclear given that the Supreme Court has never struck down a law on that basis,¹⁰⁴ but numerous lower courts have referenced the right when limiting access to intimate information in legal proceedings.¹⁰⁵ In practice, the right shows up as courts balance the informational needs of the requesting party against the privacy protection claimed by the opposition. All but one appellate court addressing the issue recognized an informational privacy right that played a role in protecting the litigants’ information from disclosure.¹⁰⁶ The right is one of general applicability and is not limited to the context of abortion, though *Whalen* itself involved medical information.

The Court in *Whalen* considered a New York law requiring physicians to report detailed information regarding the prescription of Schedule II drugs on a form identifying “the

⁹⁸ *Id.* at 2237 (citing *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977)).

⁹⁹ For a thorough discussion of the implications of Justice Alito’s reference to *Whalen*, see Shachar & Zubrzycki, *supra* note 24.

¹⁰⁰ *Nat’l Aero. & Space Admin. v. Nelson*, 562 U.S. 134, 141 (2011).

¹⁰¹ *Id.* at 138.

¹⁰² *Nixon v. Adm’r of Gen. Servs.*, 433 U.S. 425 (1977).

¹⁰³ *Nelson*, 562 U.S. at 159.

¹⁰⁴ See Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 CORN. L. REV. 1875, 1927-28 (2020).

¹⁰⁵ See Shachar & Zubrzycki, *supra* note 24, at 12-14 (detailing various cases that utilized a right to informational privacy to restrict access during discovery disputes).

¹⁰⁶ *Id.* at 4.

prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient,” though public disclosure of patient identities was prohibited.¹⁰⁷ The plaintiffs (which included physicians and patients) argued that the mandatory reporting law violated their interests in both avoiding disclosure of personal information and in making important decisions.¹⁰⁸ Plaintiffs raised the concern that disclosure of the reported information could negatively impact their reputations and, as a result, they would be discouraged from seeking out treatment or making the decision to use the controlled substances. As such, the “making of decisions about matters vital to the care of their health [was] inevitably affected by the statute.”¹⁰⁹

Although the Court ultimately upheld the statute, it did not balk at assessing the matter through the lens of prior cases “protecting ‘privacy’” that “involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.”¹¹⁰ In the end, the Court held that the statute did not “pose a sufficiently grievous threat to either interest to establish a constitutional violation.”¹¹¹ The Court did not use strict scrutiny to arrive at this result; rather, Justice Stevens highlighted the speculative nature of the concerns regarding public disclosure and noted that even if some patients were discouraged from seeking out care, many prescriptions were still being written and the state was not preventing patients from making the decision to seek care.¹¹²

As mentioned, while *Whalen* and the later *NASA* case do not establish a right to informational privacy with the strongest of Constitutional foundations, the right has been relied upon frequently by lower courts when protecting litigants’ information in discovery. In some sense, protecting personal information on the civil side extends naturally from the Court’s jurisprudence

¹⁰⁷ *Whalen v. Roe*, 429 U.S. 589, 593-94 (1977).

¹⁰⁸ *Id.* at 599-600.

¹⁰⁹ *Id.* at 600.

¹¹⁰ *Id.* at 599-600.

¹¹¹ *Id.* at 600.

¹¹² *Id.* at 600-03.

involving Fourth Amendment search and seizure in the criminal context.¹¹³ And importantly, the Court has recognized the especially sensitive nature of medical information on multiple occasions.

In *Ferguson*, for example, the Court considered the permissibility of a police protocol pursuant to which, without a warrant, hospitals were required to turn over to law enforcement the results of positive drug screenings performed on pregnant women.¹¹⁴ The Court held that the protocol was inconsistent with the Fourth Amendment¹¹⁵ and, in doing so, expressly drew attention to the fact that “[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.”¹¹⁶

More recent cases reflect a similar willingness of the Court to recognize the unique nature of medical information in emphasizing the need for a warrant to access such data. In *Riley v. California*, the Court noted that information one has on their phone is “qualitatively different” from other information and could include searches for disease symptoms or “frequent visits to WebMD.”¹¹⁷ Similarly, the *Carpenter* case referenced in Part I, that limited the reach of third-party doctrine, saw Chief Justice Roberts’s majority opinion acknowledging that “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, *doctor’s offices*, political headquarters, and other potentially revealing locales.”¹¹⁸ Roberts indicated that analysis of third-party doctrine requires consideration of “the nature of the particular documents sought,” which further opens the door for consideration of the sensitive nature of health

¹¹³ See Larry J. Pittman, *The Elusive Constitutional Right to Informational Privacy*, 19 NEV. L.J. 135, 167-68 (2018); Shachar & Zubrzycki, *supra* note 24, at 24 (highlighting that Justice Scalia favored adherence to Fourth Amendment principles in this context, because he was critical of the Court’s privacy discussion in *Whalen*).

¹¹⁴ *Ferguson v. City of Charleston*, 532 U.S. 67, 67-68 (2001).

¹¹⁵ U.S. CONST. amend. IV.

¹¹⁶ *Ferguson*, 532 U.S. at 78.

¹¹⁷ *Riley v. California*, 573 U.S. 373, 395-96 (2014).

¹¹⁸ *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (emphasis added).

information.¹¹⁹ Indeed, the majority of courts to consider the issue have found that individuals have a reasonable expectation of privacy in their medical information.¹²⁰

In sum, even as the Court's decision in *Dobbs* weakens claims for a decisional privacy right, Alito's express (and, over the years, repeated) affirmation of a distinct "right to shield information from disclosure"¹²¹ opens the door for greater protection of sensitive information. This is particularly important given the lack of a comprehensive data privacy framework. And as amorphous as a right to informational privacy may appear, the Supreme Court has consistently identified health information as particularly worthy of protection.¹²² Even still, given that the scope of any such right remains ill-defined,¹²³ further protection could be afforded by recognition of a clearly articulated privilege associated with the medical information users share with mHealth apps.

The Court's reference to a right of informational privacy is certainly consistent with the existence of evidentiary privilege. After all, "[t]he principal means of protecting confidentiality in court proceedings is through the invocation of evidentiary privileges."¹²⁴ Part III provides background on privilege doctrine

¹¹⁹ See Ryan Knox, *Fourth Amendment Protections of Health Information After Carpenter v. United States: The Devil's in the Database*, 45 AM. J.L. & MED. 331, 346 (2019) (citing *Carpenter*, 585 U.S. at 314 (citing *United States v. Miller*, 425 U.S. 435, 442 (1976))). The Court's recent decisions in *Birchfield v. North Dakota* as well as *Maryland v. King* draw particular attention to genetic information that can be distilled from DNA obtained by law enforcement. See Shachar & Zubrzycki, *supra* note 24, at 23-24 (analyzing *Birchfield v. North Dakota*, 579 U.S. 438 (2016), and *Maryland v. King*, 569 U.S. 435 (2013)). See also Jonathan F. Will, Comment, *DNA as Property: Implications on the Constitutionality of DNA Dragnets*, 65 U. PITT. L. REV. 129, 142-43 (2003) (discussing the types of information contained in DNA and arguing that recognition of a property right would strengthen the argument that a warrant is required before DNA is obtained by law enforcement).

¹²⁰ See Knox, *supra* note 119, at 346 n.138 (listing numerous such cases).

¹²¹ *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 273 (2022).

¹²² As Professors Shachar and Zubrzycki detail in their article, lower courts tend to agree when limiting access to health information in discovery disputes. Shachar & Zubrzycki, *supra* note 24, at 25-33.

¹²³ Edward J. Imwinkelried, *The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges*, 83 B.U. L. REV. 315, 327 (2003) (noting that many "courts have candidly acknowledged that the 'contours' of the right are 'murky' and 'unclear'").

¹²⁴ Lininger, *supra* note 25, at 706.

and argues that the normative justification for privilege protection supports expansion to include communication with mHealth apps.

III. PRIVILEGED COMMUNICATION WITH MHEALTH APPS

The existence of a privilege shields covered communication from being used as evidence and can also be wielded as “a basis for objecting to subpoenas, discovery requests, and deposition questions.”¹²⁵ By definition, the information contained in the conveyance is not kept strictly private by the conveyor; rather, the information is shared with a given professional such as an attorney, physician, psychotherapist, or clergy member for the purpose of seeking advice or counsel.¹²⁶ The disclosure within the relationship carries with it an expectation of confidentiality and, indeed, such professionals are ethically bound to maintain such confidence.¹²⁷ Thus, the patient or client can be confident that the information shared with professionals will not be used in later litigation.

This is true notwithstanding the fact that a given piece of litigation may proceed more efficiently if there was visibility into the discussions between, for example, a client and attorney. But the general view is that society as a whole benefits from the free exchange of information within certain relationships.¹²⁸ Simply put, clients and patients may not fully disclose pertinent information if they fear it will not be kept private. Without full disclosure, attorneys and physicians would not be able to provide the best consultation possible, which would leave all clients and patients worse off. In this way, any perceived benefit with respect to a specific legal case gives way to broader societal interests.¹²⁹

¹²⁵ *Id.*

¹²⁶ *Id.*

¹²⁷ The Oath of Hippocrates, which has retained its legitimacy for 2,500 years and is recited at medical school graduations across the country, demands that physicians hold patient information private. *See, e.g.,* Rachel Hajar, *The Physician's Oath: Historical Perspectives*, 18 HEART VIEWS 154, 156 (2017). Similarly, Rule 1.6 of the Model Rules of Professional Conduct, which have been adopted in most jurisdictions, states that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” MODEL RULES OF PRO. CONDUCT r. 1.6 (A.B.A. 2009).

¹²⁸ Lininger, *supra* note 25, at 716.

¹²⁹ Of course, the privilege would not apply if a plaintiff put the subject of the communication at issue in the litigation, such as in a legal or medical malpractice cause of action. *See, e.g.,* MISS. R. EVID. 502(d)(3), 503(e).

The development of privilege doctrine owes much to John Henry Wigmore's early (and expansive) treatises on evidence law.¹³⁰ Many of the original volumes are outdated, but the influence of Wigmore's foundational justification for evidentiary privileges persists.¹³¹ Based on instrumental theory, Wigmore started from the "behavioral assumption" that a client or patient would not fully divulge information to an attorney or physician without the "assurance of confidentiality" provided by an evidentiary privilege.¹³² And there is a societal interest in promoting communication within certain relationships, "which in the opinion of the community ought to be sedulously fostered."¹³³

From one viewpoint, there is much to gain and little to lose by recognizing privilege. Society benefits from open communication within covered relationships, and the legal system loses little if we assume that communication would not be made but for the privilege. That is, without the comfort of the privilege, the information would not have been shared in the first place and thus would not be available as potential evidence.¹³⁴ But for Wigmore, this also meant that the privilege should exist in limited circumstances. If the person would disclose the information in the absence of a privilege, then no privilege should attach. Indeed, Wigmore thought it would be rare for a sick person to withhold information from a physician, which suggests that the privilege would have modest application in the context of physician-patient communications.¹³⁵

Although instrumental theory has been endorsed as a justification for privilege doctrine by the Supreme Court,¹³⁶ it is not immune to critique. Strict adherence to a "but for" relationship

¹³⁰ Imwinkelried, *supra* note 123, at 316-17. Professor Imwinkelried was asked to revise the volume associated with privilege.

¹³¹ *Id.* at 317 (first citing *Jaffee v. Redmond*, 518 U.S. 1 (1996); and then citing *Swidler & Berlin v. United States*, 524 U.S. 399 (1998)) (noting that the Supreme Court's two most recent decisions pertaining to privilege rely heavily on Wigmore's theory).

¹³² *Id.*

¹³³ *Id.* (quoting 8 JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE § 2285, at 527 (McNaughton rev. 1961)).

¹³⁴ See *Jaffee v. Redmond*, 518 U.S. 1, 12 (1996) (noting that "[w]ithout a privilege, much of the desirable evidence . . . is unlikely to come into being").

¹³⁵ Imwinkelried, *supra* note 123, at 319 (citing 8 WIGMORE § 2380a, at 830).

¹³⁶ *United States v. Zolin*, 491 U.S. 554, 562 (1989).

between the privilege and disclosure would not seem to justify the penitent-priest protection that Wigmore himself endorsed. Catholics, for instance, may fear the eternal consequences of failure to confess sins, which would lead them to disclose information even in the absence of an evidentiary privilege.¹³⁷ This calls into question the “but for” justification for acknowledging privilege; that is, that the privilege should exist only where the information would not be disclosed but for the evidentiary protection in litigation.

A more practical deficiency of instrumental theory is that it presumes that people think about (and organize their behavior in anticipation of) litigation more than they actually do.¹³⁸ While the lives of attorneys and judges might be shaped by frequent thoughts of litigation, projecting that onto the lay populace proves too much. Instead, “[l]aypersons consulting professionals appear more concerned about unauthorized, out-of-court revelation to third parties such as employers and insurers than about court-supervised disclosure.”¹³⁹

It seems unremarkable that laypeople do not structure their lives with reference to the laws of evidence, and the Congressional deliberations associated with the initial adoption of the Federal Rules of Evidence acknowledge this.¹⁴⁰ In short, the “but for” behavioral assumption associated with instrumental theory is too narrow to serve as the sole normative justification for the privilege doctrine. Though Wigmore himself may have felt that a physician-patient privilege would have limited application, a more comprehensive view of the goals achieved by recognizing privilege lays the groundwork for expanding privilege to cover communications with the mHealth apps that individuals have come to rely upon.

Long before Wigmore wrote about evidence, ancient physicians turned to the ethical precepts set forth in the Oath of Hippocrates.¹⁴¹ Even its modern variations, which are recited at

¹³⁷ Imwinkelried, *supra* note 123, at 321.

¹³⁸ EDWARD J. IMWINKELRIED, *THE NEW WIGMORE: A TREATISE ON EVIDENCE* § 5.2.2 (2002).

¹³⁹ Imwinkelried, *supra* note 123, at 322.

¹⁴⁰ *Id.* at 322-23.

¹⁴¹ Hajar, *supra* note 127, at 156.

medical school graduations across the country to this day, include the principle that physicians should maintain their patients' privacy.¹⁴² While this ancient text may not have carried the weight of law, preserving such confidence has always been considered paramount to ensure the full and accurate disclosure of information necessary for proper treatment. Indeed, it is more likely that patient awareness of this norm would provide the comfort necessary to fully disclose intimate information than a backend litigation privilege.

To be sure, the early physician-patient relationship was not known for an active decision-making role for patients. Historically, physicians would unilaterally choose the treatment thought most beneficial,¹⁴³ but patients would still have needed to honestly and accurately describe their symptoms for the physician to make that determination. That type of open communication within certain relationships has long been a justification for evidentiary privilege.

Today, a further normative justification exists. Informed consent doctrine in the United States developed alongside the Bioethics Movement in the middle of the twentieth century.¹⁴⁴ Consistent with Western liberal tradition, patients came to be recognized as autonomous agents deserving of respect as such.¹⁴⁵ Physicians, as fiduciaries, have an obligation to facilitate the process by supplying the information material to the patient in making the medical decision at hand.¹⁴⁶

In this way, promotion of autonomous decision-making within the relationship becomes its own objective, and recognition of an evidentiary privilege supports that aim. As Professor Imwinkelried notes, "[a] liberal democratic state should assure its

¹⁴² *Id.*

¹⁴³ See generally Jonathan F. Will, *A Brief Historical and Theoretical Perspective on Patient Autonomy and Medical Decision Making, Part I: The Beneficence Model*, 139 CHEST 669 (2011) (discussing the one-sided nature of early physician-patient interactions).

¹⁴⁴ See generally Jonathan F. Will, *A Brief Historical and Theoretical Perspective on Patient Autonomy and Medical Decision Making, Part II: The Autonomy Model*, 139 CHEST 1491 (2011) (describing how the law of informed consent and the Bioethics Movement gave rise to a more active role for patients in the decision-making process).

¹⁴⁵ *Id.* at 1496.

¹⁴⁶ *E.g., Canterbury v. Spence*, 464 F.2d 772, 786-87 (D.C. Cir. 1972).

citizens that they may enter into intimate consultative relationships with minimal risk that their autonomy will be violated during the consultation. To accomplish this, the state must create conditions conducive of trust,”¹⁴⁷ which is exactly what privilege protection does. The value of the recommendation given by the physician is necessarily correlated with the honesty and accuracy of the information supplied by the patient. Through privilege protection, society fosters an environment where autonomy thrives due to the free exchange of information that enables patients “to make better-informed, more independent choices among medical options.”¹⁴⁸

The nature and scope of any physician-patient privilege is generally determined by individual states.¹⁴⁹ For example, Mississippi Rule of Evidence 503 establishes a “Privilege between Patient and Physician or Psychotherapist.”¹⁵⁰ Patient is defined as “a person who consults, is examined by, or is interviewed by a physician or psychotherapist,” and both physician and psychotherapist are defined with reference to a licensed “person” involved in diagnosis and treatment.¹⁵¹ The advisory committee notes to Rule 503 indicate that Mississippi statutory law expands the privilege to include communications with osteopaths, dentists, hospitals, nurses, pharmacists, podiatrists, optometrists, and chiropractors.¹⁵²

On its face, Rule 503 is limited to communications with “person[s]” involved in the patient’s diagnosis or treatment but would include any “knowledge the physician or psychotherapist

¹⁴⁷ Imwinkelried, *supra* note 123, at 333.

¹⁴⁸ *Id.* at 338. The privilege protects the physician as well by allowing open discourse about divisive treatment options without fear of public backlash. *Id.* at 336-37.

¹⁴⁹ Melissa O’Neill, Note, *Ohio’s Patient-Physician Privilege: Whether Planned Parenthood Is a Protected Party*, 17 J.L. & HEALTH 297, 309-12 (2002) (discussing Ohio’s approach to defining physician, patient, and communication in the context of the privilege). The Federal Rules of Evidence do not include a general physician-patient privilege, though the Supreme Court recognized a psychotherapist-patient protection in *Jaffee v. Redmond*, 518 U.S. 1, 15 (1996). The rationale used in *Jaffee* supports the expansion of privilege protection to include communication with health tracking apps. See *infra* notes 163-166 and accompanying text.

¹⁵⁰ MISS. R. EVID. 503.

¹⁵¹ *Id.* § 503(a)(1)-(3).

¹⁵² See MISS. CODE ANN. § 13-1-21 (2026).

derived from the professional relationship with the patient.”¹⁵³ The rule is also broad enough to pick up certain communications not made directly to the physician. That is, such communications remain confidential if:

(A) made for the purpose of diagnosing or treating the patient’s physical, mental, or emotional condition, including alcohol or drug addiction, and

(B) between or among the patient, the patient’s physician or psychotherapist, and persons—including the patient’s family—participating in the diagnosis or treatment under the direction of the physician or psychotherapist.¹⁵⁴

The privilege is for the patient to claim but may be asserted by the physician, psychotherapist, or other professional on the patient’s behalf.¹⁵⁵

Because the text of the rule is tied to communication with “persons” in an existing professional-patient relationship, it is unlikely to be read to include information conveyed in mHealth apps absent an amendment or clear judicial interpretation to that effect. Perhaps the most straightforward circumstance would be where the patient utilizes an mHealth app at the direction of a health care professional as part of the treatment or diagnostic plan. In that case, the app may already be covered by HIPAA.¹⁵⁶ But the justification supporting privilege points to a more expansive view.

After all, the rationale for privilege is not primarily focused on the audience/professional. The protection typically must be raised and can only be waived by the patient.¹⁵⁷ The aim is ultimately to empower people to make decisions for themselves, thereby respecting them as autonomous agents.¹⁵⁸ Professor Lininger aptly points out that privilege should depend “on the

¹⁵³ MISS. R. EVID. 503(b)(1).

¹⁵⁴ *Id.* § 503(b)(2).

¹⁵⁵ *Id.* § 503(c).

¹⁵⁶ See *supra* notes 59-61 and accompanying text.

¹⁵⁷ The advisory committee notes to Rule 503(c) explicitly state that “[s]ubdivision (c) is reflective of M.C.A. § 13-1-21. The privilege belongs to the patient, and only the patient can waive it.” MISS. R. EVID. 503 advisory committee’s note.

¹⁵⁸ Imwinkelried, *supra* note 123, at 333-36.

subject matter of the communication—not the credentials of the audience.”¹⁵⁹ This is especially true for “[l]ow-income and minority populations,” who, statistically, have had less access to and more skepticism toward the categories of professionals to whom the privileges typically apply.¹⁶⁰

The preamble language to evidence and ethics rules alike speak to the promotion of fairness,¹⁶¹ and privilege protection ought to apply equally to all. As individuals are encouraged to take more active roles in their health and, in turn, to rely on apps to assist with their progress, it becomes imperative to ensure that the information shared with these mHealth apps is complete and accurate.¹⁶² The apps become one more tool, in addition to (or sometimes in place of) health care professionals, that are designed to allow autonomous individuals to realize their health potential.

This more expansive view of privilege is consistent with the rationale provided by the Supreme Court in *Jaffee v. Redmond*.¹⁶³ There, the Court determined that the psychotherapist-patient privilege included in the Federal Rules of Evidence extends to social workers who provide mental health treatment as well.¹⁶⁴ Importantly, the Court highlighted the “public interest” served by virtue of how privilege protection “facilitat[es] the provision of appropriate treatment.”¹⁶⁵ The Court reasoned that expanding the privilege to include social workers was important because their clients “often include the poor and those of modest means who could not afford the assistance of a psychiatrist or psychologist”¹⁶⁶ (those to whom the privilege traditionally applies). The Court’s language is sensitive to the fact that promotion of health is a societal benefit, and it is reasonable to extend the privilege in ways that facilitate those goals. Because social workers providing

¹⁵⁹ Lininger, *supra* note 25, at 720.

¹⁶⁰ *Id.* at 670.

¹⁶¹ *Id.* at 720.

¹⁶² *See supra* Part I.

¹⁶³ 518 U.S. 1 (1996).

¹⁶⁴ *Id.* at 15.

¹⁶⁵ *Id.* at 11.

¹⁶⁶ *Id.* at 16.

psychotherapy serve similar societal goals as psychiatrists, the Court had “no hesitation” expanding the privilege.¹⁶⁷

Although not all interactions with mHealth apps necessarily involve diagnosis or treatment, the apps play an instrumental role in allowing individuals to monitor their health and wellbeing. This, in turn, allows them to fully recognize their potential as autonomous agents, which provides both individual and public health benefits.¹⁶⁸

As previously mentioned, improperly managed chronic illness is a leading cause of death and medical expense worldwide, and there remains a lack of research into menstrual health. mHealth apps allow individuals to take a more active role in maintaining their wellbeing, and this is true regardless of whether the app is utilized at the express direction of a physician. In any circumstance the effectiveness of the app is proportional to the accuracy and completeness of the intimate information entered. Recognizing privilege protection for such information is a step toward facilitating these health goals and is consistent with what other scholars have termed a self-surveillance privilege.¹⁶⁹

Even still, privileges can be waived. For instance, mHealth app users would need to be vigilant to avoid waiving the privilege by consenting to the sale of their information. That said, if app developers make it difficult for individuals to opt out of the sale of their data (for instance, by burying consent in hard-to-find terms and conditions)¹⁷⁰ that fact should be relevant to any waiver analysis. But inputting information into the app alone should not constitute a waiver, and the unauthorized sale of data to third parties should never be considered a waiver. Further, information shared in an mHealth app that is de-identified prior to an authorized sale, but which is subsequently re-identified, should retain privilege protection in any future civil or criminal litigation.

Privilege protection is also not absolute. After all, medical records can be subpoenaed as part of a criminal investigation, and

¹⁶⁷ *Id.* at 15. For an argument that privilege could extend to communications between a patient and Planned Parenthood, see O'Neill, *supra* note 149.

¹⁶⁸ O'Neill, *supra* note 149, at 319-20.

¹⁶⁹ Kang et al., *supra* note 27, at 832, 835.

¹⁷⁰ For instance, the European Union's comprehensive General Data Protection Regulation ("GDPR") "warns . . . that '[s]ilence, pre-ticked boxes or inactivity should not . . . constitute consent.'" Tovino, *supra* note 1, at 183 (alteration in original).

there may be overriding laws that require confidentiality to be breached when necessary to prevent future harm.¹⁷¹ But the privilege could be wielded to prevent disclosure in civil and criminal actions or, at the very least, to make the data more difficult to obtain. Severe backend restrictions on the use of the information would make it less attractive, and that alone may reduce efforts to access the data on the front end.¹⁷² Chilling those who would otherwise actively seek such intimate data is a worthwhile end in itself.

CONCLUSION

Keeping data private is increasingly difficult at a time when the United States lacks a comprehensive privacy framework. This is particularly true given the tremendous market for consumer information. As individuals increasingly turn to mHealth apps, including CTAs, to assert more control over their wellbeing, intimate health information is put at risk. While unsolicited advertisements may be a minor nuisance, the threats are more significant when the information is used by interest groups or law enforcement.

Because any Constitutional right to informational privacy remains ill-defined, the law ought to recognize an evidentiary privilege protecting the information people share with mHealth apps. The normative justification for privilege doctrine—to promote autonomous decision-making through open communication—applies with equal force as individuals share intimate health data with the mHealth apps on which they have come to rely.

¹⁷¹ Lininger, *supra* note 25, at 708-09; Fowler & Ulrich, *supra* note 10, at 1257.

¹⁷² Lininger, *supra* note 25, at 723-24.