UVA | FRANK BATTEN SCHOOL of LEADERSHIP and PUBLIC POLICY

DATA MINING OF FERTILITY TRACKING APPS

PREPARED FOR :

SENATOR GHAZALA HASHMI

GHAZALA
HASHMI
VIRGINIA SENATE

DEDICATION

I would like to dedicate this report to the loving memory of my dad, David S. Bruce. Thank you for teaching me to think critically, to embrace nuance, and always to remain curious.

ACKNOWLEDGEMENTS

There are many people I would like to thank for my APP. First, Senator Hashmi, for this incredible opportunity to work together. You have been an amazing legislator, and it is an honor to assist you in this work. Thanks also to June Laffey, Senator Hashmi's Chief of Staff, for coordinating and communication.

Thank you to my teachers and mentors who helped make this a success. Professor Andrew Pennock, thank you for keeping me on task. You transformed this topic from a fledgling idea to a fully formed research paper. Thanks also to Professor Joel Schlosser from Bryn Mawr. You first awakened my interest in the practice of policymaking.

Senator Elizabeth Warren, thank you for being a tireless consumer advocate and inspiring me to go to grad school.

Thank you to all of my friends who took the time to listen and give me feedback on my work: Sam, Will, Javier, Toby, Liv, Ryan, and Danny. Of course, thanks to my mom. I could not have done this without you.

DISCLAIMER

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

HONOR STATEMENT

On my honor as a University of Virginia student, I have neither given nor received unauthorized aid on this assignment.

TABLE OF CONTENTS

I Glossary 1

II Executive Summary 2

III Introduction & Problem Statement 3

IV Client Overview 4

V Background 5

VI Recommendation 12

VII Adoption 18

VIII Implementation 21

IX Appendix 22

X Works Cited 24

GLOSSARY

Consumer Generated Data (CGD) = Data created by consumers, which includes geolocation, behavioral health data, finger patterns, or any other data collected by apps.

Personal Health Information (PHI) = Data primarily collected by covered entities, usually includes measurements of health like blood pressure, weight, height, or notes from a healthcare provider.

Health Information Portability Accountability Act (HIPAA) = The law defines the privacy rights of a patient regarding their PHI. Requires covered entities to maintain certain standard of data security.

Covered Entities = Health care providers, health insurance companies, health care clearinghouses, and their business associates.

First party data collectors = Organizations that collect, maintain, or sell CGD from the vehicle it was generated in (e.g. phone apps, web-browsers).

Data Brokers = Also can be described as third parties, primarily buy, sell, or harvest data from consumers.

Regulated Entities = Both first- and third-party data collectors.

Data Mining = The practice of buying, selling, inferring, or harvesting CGD for profit.

Bruce I

EXECUTIVE SUMMARY

In June 2022, the Supreme Court effectively overturned abortion legalization in the Dobbs v. Jackson Women's Health Organization ruling. In 13 states, 'trigger laws' went into effect, immediately criminalizing abortion. While Virginia has been a haven for abortions, the election of an anti-abortion Governor and recent flip of the House of Delegates puts this status in a more precarious position.

After Dobbs, one of the stories circulating in the news and social media was the revelation that the data from fertility tracking apps—apps used by people to track their reproductive health—was being sold and provided to law enforcement prosecuting people pursuing abortions. In these cases, the prosecution will use data from fertility tracking apps managed as evidence in the case. One potential policy intervention to protect this vulnerable group of people is to implement stricter data privacy laws at the state level.

In this research paper, the problem is framed as the data privacy problem within the abortion conversation. Legislative efforts to protect abortions have been blocked by the House and the Governor. However, implementing stricter data privacy laws can be a roundabout way of legislating abortion protections. This paper attempts to synthesize the relevant information in the field of data privacy. Given the complexity of this topic, the intention of this paper is to provide not just a policy recommendation, but additional background and understanding of the necessary provisions.

The report is divided into four main sections: history of data privacy, the mechanics of different potential policies, the policy recommendation, and adoption strategies. The alternatives will be analyzed by the following criteria: dignity, equity, political feasibility, and administrative feasibility.

My recommendation for the Senator is to adopt a plan like the Washington State Data Health Privacy bill and an anti-discrimination clause. This bill scores the highest on all four criteria by offering the most protections to consumers. Coupled with this strategy, I recommend the Senator package this bill in a way to emphasize libertarian values of autonomy and privacy to win over her Republican colleagues.

INTRODUCTION

Every time a person with a menstrual cycle goes to the doctor, one of the first questions the doctor asks is: “when was the last day of your most recent period?” They ask this question because periods are a method of measuring health and wellness. Delayed periods can indicate underlying health problems and are frequently correlated with certain illnesses. Until recently, people primarily used analogue forms to track cycles like a journal to answer this question. The digital era has replaced these analogue instruments with fertility-tracking apps. However, unlike the journal, the information stored on these apps is not completely private.

In the digital era, apps provide many benefits and ease for the consumer. They streamline and optimize systems of communication and organization. However, these perceived eases come at the cost of personal privacy. In the case of using a fertility-tracking app, a person might be spending a relaxing evening at home watching TV when an advertisement for baby formula appears. They realize it’s been a while since their last period. They check their app, and it has been 45 days. It seems like a weird coincidence or something out of a sci-fi novel, but it is the new reality for many users.

Recently, it became clear that the makers of these apps collect and sell this data to third parties for profit. Politico identified 30 data brokers that tracked the names and addresses of expecting parents. One of them, Exact Data, sells the birth dates for 28,000 babies, updating the names monthly (Ng, 2022). Gizmodo found 32 data brokers who were selling the contact information of 2.9 billion pregnant users, setting the price per user between 49 cents to $2.25 (Wodinsky & Barr, 2022). This poses risks to consumers because the market for selling this data is not regulated at all. Health data, reproductive health data in particular, can be exploited and lead to discrimination and criminalization.

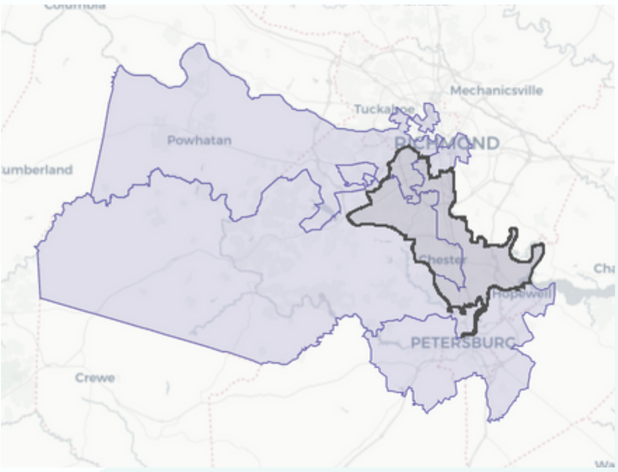
PROBLEM STATEMENT

In the post-Dobbs era, fertility-tracking apps pose great risks to people seeking abortions. Users of these apps are unknowingly forfeiting their right to intimate privacy, the consequences of which could be employment discrimination, health care discrimination, and lawsuits against people seeking an abortion. Given the lack of federal regulation of this issue, the stakes are higher than before. There is an opportunity to increase user protections by implementing data privacy legislation at the state level.

CLIENT OVERVIEW

My client is Virginia State Senator Ghazala Hashmi, who was elected to office since 2019. Before holding political office, she was a professor of English at Reynolds Community College. Her husband is a researcher at VCU, and she has two daughters, both of whom are UVA graduates. Her campaign was endorsed by NARAL and Planned Parenthood. She ran on a platform of protecting reproductive freedom and increasing access to medical care. Protecting reproductive health data is something she's passionate about in part because of its implications for her communities, which are now more vulnerable in a post-Dobbs landscape.

Senator Hashmi currently represents parts of Richmond, Chesterfield County, and all of Powhatan County. With redistricting, she is seeking reelection in a district made up of parts of Richmond and Chesterfield County. After redistricting, her district is D+18. so it is unlikely to be a competitive election. This gives her a lot of leeway in terms of proposing liberal legislation without concern of re-election capacity. She serves on the Joint Committee on Technology and Science and the Joint Commission on Health Care, two bodies relevant to this research.



(Black line represents new boundaries of district, source: vpap.org)

BACKGROUND

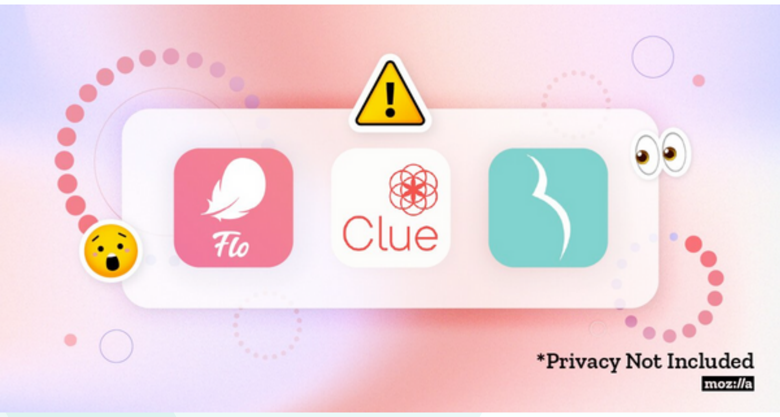
LEGAL DISTINCTIONS BETWEEN PHI AND CGD

9%

OF USERS READ THE PRIVACY POLICY BEFORE AGREEING TO THE TERMS AND CONDITIONS

American data privacy law is largely based on notice and consent (Solove & Hartzog, 2013). For many years, the "consent" framework has been largely broken, as users opt into the privacy policy without an informed view of what they are consenting to. Only 9% of users read their apps privacy policy before agreeing to the terms and conditions (Auxier et al., 2019). Additionally, the user is responsible for the care of their personal data by themselves and by the parties who collect it, even in the incident of a data breach by regulated entities. There are few mechanisms for them to delete data from the app companies once shared by the user (Gilman, 2021).

A growing area of concern is the health care app industry, which collects consumer health data from app users and sells it to advertisers for a profit. This technology has created new vulnerabilities around security of personal data. Companies like Meta that have sold user-facing apps to hospitals have leaked millions of data points concerning sensitive health information of its users (Feathers & Fondrie-Teitler, 2022). Market forecasters predict the Femtech industry, which profits from apps for regulating female health, will gross $50 billion by 2025 (Frost & Sullivan, 2018). A large group of these apps collect data on menstrual cycles, which are popular among people with irregular cycles such as post-partum parents, athletes, and people with Polycystic Ovarian Syndrome (Rosato, 2020).

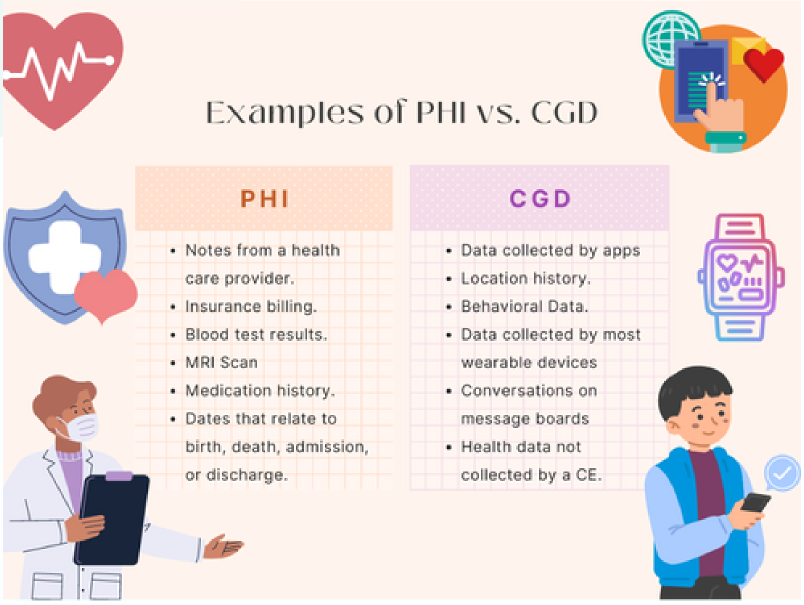


The Mozilla Foundation found 18 of 25 Popular Period Tracking Apps did not have responsible data privacy practices

BACKGROUND

LEGAL DISTINCTIONS BETWEEN PHI AND CGD

Even before Dobbs, data from apps have been used to criminalize people (Elliott, 2022). Fertility app data could also fuel the criminalization of birth control, which some states have also attempted to outlaw post Dobbs (Ollove, 2022). Many users incorrectly assume that these apps are protected by HIPAA, which regulates mostly Personal Health Informaiton (PHI). There is not a legal term for data on consumer apps, so I've named it Consumer Generated Data (CGD) for this report. The table below explains their differences.



Examples of PHI vs. CGD

PHI	CGD
• Notes from a health care provider. • Insurance billing. • Blood test results. • MRI Scan • Medication history. • Dates that relate to birth, death, admission, or discharge.	• Data collected by apps • Location history. • Behavioral Data. • Data collected by most wearable devices • Conversations on message boards • Health data not collected by a CE.

Table: Authors own interpretation

KEY FACTS

HIPAA sets minimum data security standards covered entities (health care providers, health insurance companies, and their business associates). This does not include most health apps.

Out of all the federal agencies, the FTC is best positioned to address consumer data privacy issues, because the issue falls under the institutional mandate to prohibit "unfair and deceptive practices." (Mission, 2021).

One potential intervention to this problem is to encourage covered entities to develop their own apps. Data privacy expert Justin Sherman explained this would continue to play into the current problems around privacy. Insurance companies themselves also buy data and sell about consumers. The key difference is that covered entities are required to remove 17 unique identifiers defined by HIPAA statute. However, it is relatively not difficult for data brokers to re-identify the consumer. Ultimately, HIPAA's statute was not written with our current data privacy ecosystem in mind. Another one of the undesirable effects is that covered entities are not required to disclose to consumers what third parties they share information with once it is de-identified.

HISTORY OF THE LEGAL RIGHT TO PRIVACY

The “Right to Privacy” was not established in the Constitution, but rather created by two lawyers. In 1890, tabloids surged in popularity, unearthing the skeletons of public figures. During this period, Samuel D. Warren was an attorney in private practice in Boston. He feared the tabloids would uncover his brother’s closeted homosexuality and ruin his family’s reputation and brother’s life. He asked his law partner and future supreme court Justice, Louis Brandeis, to write a law review article with him on the “right to privacy.” He hoped this would scare away journalists because of perceived potential legal recourse. They were lauded for their article, and almost overnight, privacy was assumed to be a legal right (Citron, 2022).

US LEGISLATIVE HISTORY

- The Privacy Act of 1974: established rules and procedures for federal agencies collecting personally identifiable information.
- The Privacy Protection Act of 1980: provided legal protection of information for journalists against illegal searches and seizures.
- The Electronic Communications Protection Act of 1984: limited government wiretapping of phones.
- The Video Privacy Protection Act of 1988: prevented wrongful disclosure of video tape records.
- California Consumer Privacy Act of 2018: establishes digital rights for Californians including the right to delete, the right to opt-out, and the right to non-discrimination.
- American Data Privacy and Protection Act: federal data privacy legislation bill that has not passed Congress and has little promise of passing soon.

Europe’s General Data Privacy Regulation

The General Data Privacy Regulation (GDPR) is the main data privacy policy in Europe. The EU created it to streamline the different individual privacy policies of EU member states. It outlines eight rights for all users: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and the right to avoid automatic decision making (Burgess, 2020). GDPR is the gold standard of robust protections but it would be difficult to pass in the United States, largely because of Congressional gridlock. Even after the White House Office of Personnel Management was hacked, exposing the personal data of over 22 million federal employees, Congress couldn’t pass nationwide security standards (Hawkins, 2020).

HISTORY OF THE LEGAL RIGHT TO PRIVACY

Harvard Professor Shoshana Zuboff identifies three historical windfalls that enabled the rise of consumer data harvesting.

1. After 9/11, Congress dramatically shifted its attitudes of use of surveillance tools from skepticism to enthusiastic support. This tragedy gave rise to the Department of Homeland Security, the Patriot Act, and other measures that limited privacy of citizens in exchange for “protecting the homeland.”
2. Neoliberalism was the dominant school of economic thought, which emphasized the importance of letting the market self-regulate. In this environment, the government stepped back from scrutinizing the development of harvesting tools.
3. Google took advantage of this regulatory environment to create the foundational algorithms that are used to track users on the internet today. This technology gave rise to the data broker industry (Laidler, 2019).

DATA BROKER REGISTRIES

Data brokers are third parties that buy data from first parties that initially harvest the data from the apps. California and Vermont requires data brokers to register to the state. Vermont's registry requires brokers to disclose name, primary location, opt-out permissions, number of past security breaches, policy of data collection of minors. Brokers who refuse to register receive a fine.

In the last twenty years, Google and other companies have developed algorithms to predict their future consumer behavior. In 2012, The New York Times published a story about Target’s statisticians' developing the method to target new parents starting in 2002 (Duhigg, 2012). In buying consumer demographic behavior and analyzing historic purchases, they developed a “pregnancy score” that estimated the likelihood the person was pregnant as early as the second trimester. After identifying high scorers, they barraged them with ads for baby products. Their assumption was if they locked in the loyalty of a parent early, they could make them a lifelong customer. The behavioral data that predict consumer preferences became the gold of the digital era.

RULEMAKING AND ENFORCEMENT

The FTC is the primary agency that enforces consumer data privacy. The level of enforcement powers the FTC exercises depends on the Chair and its Commissioners. Its new chair, consumer advocate Lina Khan, has reinvigorated the agency by leading the charge for pro-consumer policies and litigations. The FTC recently filed a consent decree against Flo, a popular fertility tracking app, that lied to users out their practice of selling data to Facebook (Federal Trade Commission, 2021). However, compared to other federal agencies, the FTC must jump through more hurdles to pass regulation. For example, they can only file an injunction against a company for repeated violations, rather than taking first time violators or taking other proactive measures.

More frequently, states are stepping up to regulate regulated entities. Former California Attorney General Xavier Becerra sued Glow for its data sharing practices, including a security flaw that enabled third parties to access user data by resetting passwords (Becerra, 2020). Five states (California, Colorado, Connecticut, Utah, and Virginia). have all passed comprehensive consumer data privacy laws (National Conference of State Legislatures, 2022). However, the tech industry has a heavy hand in shaping state-level policy, often limiting the number of protections these laws provide consumers.

Consumer advocates criticize Virginia's data privacy bill Virginia Consumer Data Protection Act (VCDPA) for weak enforcement provisions (Hart & Zick, 2021; Moomaw, 2021; Smith, 2021). One major criticism is that the burden falls on the user to opt out of data collection practices. Because of the sheer number of regulated entities collecting data, it is a Sisyphean task to opt out of every single one. Since the law just went into effect in January of 2023, many of these weaknesses have yet to be tested and thoroughly scrutinized.

First vs. Third Party Regulation

Another important aspect of the regulatory policy Justin Sherman highlighted was the difference between laws imposed on first party and third party data collectors. First parties are the companies that develop and monitor the apps used by consumers. Third parties are the actors who buy, sell, and harvest this data. Most data privacy regulation puts restrictions only on the third parties, which provides an opportunity for the first parties to evade regulation. For example, a first party could "license" the data in exchange for payment. There are some cases however where first parties need to transfer information to third parties for functionality's sake. There will need to be further consultation with Justin Sherman and attorneys with more knowledge in the field on exact phrasing to maintain accountability without sacrificing functionality.

CONSEQUENCES OF DATA MINING

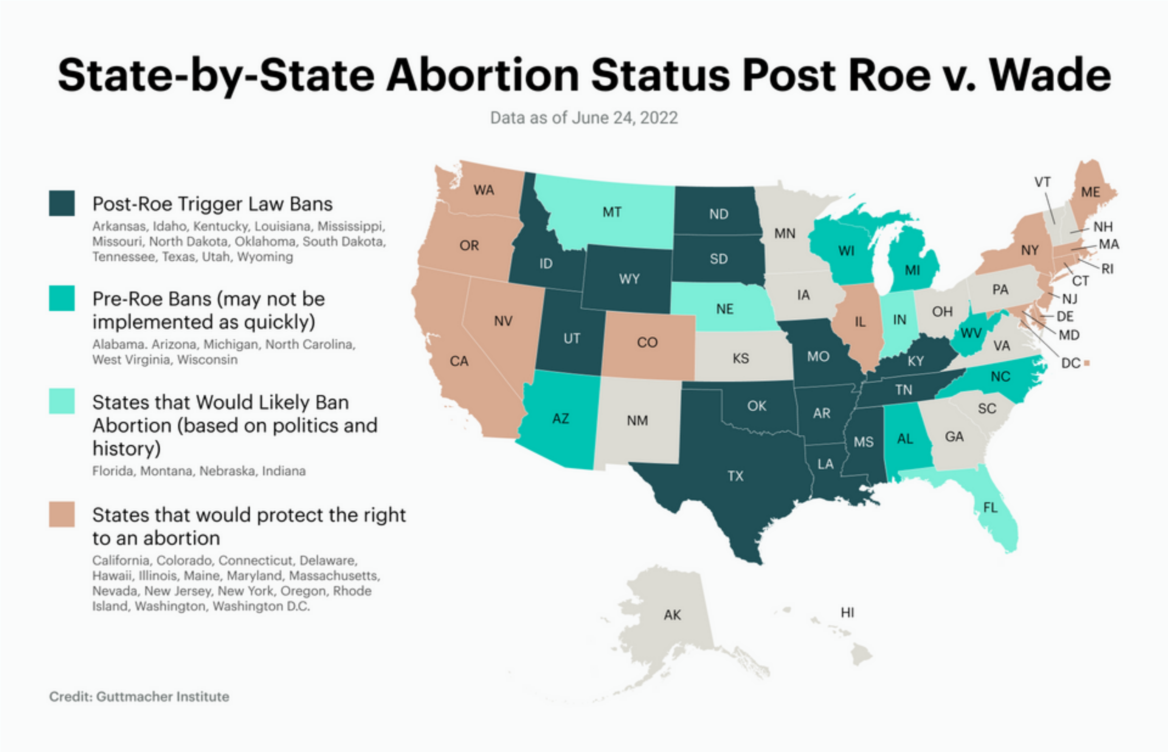
These apps were not supposed to be dangerous. The advent of health app technology was initially praised for “activating” patients. In clinical settings, activated patients tend to take more initiative in improving their health than “not activated” counterparts. In one behavioral research study, doctors gave better care to patients they perceived to be activated (Street et al., 2007). However, this perception of activation by doctors of their patients can also lead to bias.

Though there may be potential benefits in patient activation, the apps remain a questionable source for health care advice. Out of 48 apps surveyed in the mobile app store, only 11 cited a peer reviewed source (Womack et al., 2020). Some of the apps give advice using on algorithmic inferences from user generated data. They often provide flawed and poorly sourced advice on alcohol consumption and nutrition, which can have negative consequences for people seeking pregnancies (Brown et al., 2019). The presence of information in mobile apps that could potentially lead to risk seeking behavior should be of concern to healthcare providers.

Even though there is insufficient data to claim employers are actively using data to discriminate, we can infer what some of the potential realities are using research on workplace discrimination. According to the UK based Equality and Human Rights Commission’s 2018 survey, nearly half off the 440,000 pregnant women in the UK reported experiencing employment discrimination in the last year because of pregnancy. Employment discrimination can take the form of refusal to hire, being passed over for a promotion, or not being assigned to projects because of suspected parental leave. They also found around half of employers saw pregnancies to be an “undue financial cost.” (Equality and Human Rights Commission, 2018).

Perceived employment discrimination in the postpartum period is strongly correlated with lower gestational ages, lower newborn birth weights, and more frequent doctors’ visits (Hackney et al., 2021). This discrimination will disproportionately impact Black and Latinx parents, who are more likely to have chronic health problems and higher mortality rates than white parents (Sonderlund et al., 2021). Employment discrimination towards pregnant parents has serious implications for the public policy arena because of these potential negative health and economic consequences.

EQUITY IMPLICATIONS



State-by-State Abortion Status Post Roe v. Wade

Data as of June 24, 2022

Post-Roe Trigger Law Bans
Arkansas, Idaho, Kentucky, Louisiana, Mississippi, Missouri, North Dakota, Oklahoma, South Dakota, Tennessee, Texas, Utah, Wyoming
Pre-Roe Bans (may not be implemented as quickly)
Alabama. Arizona, Michigan, North Carolina, West Virginia, Wisconsin
States that Would Likely Ban Abortion (based on politics and history)
Florida, Montana, Nebraska, Indiana
States that would protect the right to an abortion
California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maine, Maryland, Massachusetts, Nevada, New Jersey, New York, Oregon, Rhode Island, Washington, Washington D.C.
WA
MT
ND
MN
OR
ID
WY
SD
WI
MI
NV
UT
CO
NE
IA
IL
IN
OH
PA
NY
VT
ME
NH
MA
RI
CT
NJ
DE
MD
DC
WV
VA
CA
KS
MO
KY
AZ
NM
OK
AR
TN
NC
SC
MS
AL
GA
LA
TX
FL
AK
HI

Credit: Guttmacher Institute

source: theskimm.com

Weak data privacy rights pose great risks to low-income and consumers of color, who rely primarily on their cell phone for access to the internet (Koepke et al., 2020). Between 2000 - 2021, there were over 60 cases of people being arrested, investigated, or charged with aiding or abetting an abortion as a criminal act. The first woman to be charged, convicted, and sentenced for “feticide” was Purvi Patel in 2015. The state had used text messages, web searches on her iPad, and emails from online drug marketplaces for abortion pills as evidence. She was sentenced to 20 years in prison but was released after the ruling was overturned for misinterpreting the state’s statute (Zakrzewski et al., 2022).

In another case, a woman in Mississippi named Lattice Fisher, was charged with second degree murder after her baby was stillborn. The prosecutors used her cell phone internet search history records as evidence. After spending a few weeks in jail, she was released when evidence surfaced that the medical examiner used unreliable methods to determine the child was born but died of asphyxiation in an autopsy. Both stories are clear examples of how people from marginalized communities can be criminalized at higher rates. Purvi Patel is an Indian woman and Lattice Fisher is a Black woman.

RECOMMENDATION

Policy	Dignity	Equity	Political Feasibility	Administrative Feasibility
Status Quo	LOW	LOW	HIGH	HIGH
Washington State Legislation	HIGH	MEDIUM	MEDIUM	MEDIUM-HIGH
Advocate Legislation	HIGH	MEDIUM-HIGH	LOW	MEDIUM

My recommendation is to adopt the **Washington state legislation,** as it ranks the highest in nearly every category. It is the “goldilocks recommendation” for hitting each of the criteria at a medium to high level. The status quo alternative is too volatile in the long term to ensure improved dignity and equity outcomes, and the advocate legislation has too many barriers to political and administrative feasibility. Reasoning for Dignity and Equity rankings included in Appendix I.

Another benefit of the Washington State legislation is that it has been recently brought through a legislative session, and the co-sponsors will be able to provide best practices and recommendations for the Senator.

An additional provision needs to be adopted to this legislation: a non-discrimination clause. This addition would increase the Equity rating from MEDIUM to MEDIUM-HIGH. A full table of all potential additional provisions to adopt to strengthen the bill is included in Appendix II.

CRITERIA DEFINITIONS

Given the complexity of measuring Dignity and Equity, I used a point system in a table available in Appendix I. A longer break down of each policy is available in Appendix II. For the Dignity and Equity criteria, I used a point system to determine **LOW**, **MEDIUM**, and **HIGH** scoring. The full table is available in appendix II.

Dignity: The Dignity criterion measures the amount of privacy it will provide users. According to UVA Law Professor Danielle Citron, the leading scholar in data privacy, dignity central to data privacy. Without this autonomy of our data, we become alien to ourselves and lose our dignity, and we can't be full members of society. A HIGH score on this criterion means significantly more protections for user data. A LOW score equates to little or uncertain change in protections.

Equity: Virginia is a state that has great income inequality and information access inequality. Low-income people are five times more likely to have an unintended pregnancy than their affluent counterparts (Reeves & Venator, 2015). Current data privacy practices operates under the "choice regime", placing responsibility on the user for data responsibility. Low-income consumers are most at risk in this regime, as they are least likely to employ common safeguards against tech and more vulnerable in a weak data privacy world (Madden et al., 2017). Additionally, even before Dobbs, Black, Brown, and low-income people were disproportionately targeted by law enforcement for pregnancy-related offenses (Paltrow & Flavin, 2013).

Political Feasibility: It is undeniable that abortion has become a political issue. Promoting legislation that would barr law-enforcement from collecting reproductive health data would be a non-starter to Republicans. Given the political environment, any feasible legislation will require bipartisan support. Recommendations ranking HIGH are very bipartisan, whereas LOW will face strong partisan opposition. MEDIUM is the middle ground; there is capacity for cooperation conditional on adoption methods.

Administrative Feasibility: The final criterion will assess what administrative hurdles may need to be addressed before the policy's implementation. This primarily measures costs of implementing the policy. The ability to bring cases against defending companies is mediated by the technical expertise and administrative capacity of the office, and a lack thereof may require additional personnel. Recommendations that rank HIGH on this criterion will be low to no cost, whereas MEDIUM and below will require an appropriation from the general budget.

ALTERNATIVE 1: STATUS QUO

The status quo is the outcome without intervention. The field of data privacy is dynamic, and the future is uncertain. As recently as February 2nd, 2023, there have been substantive changes in the data privacy landscape, with the FTC finally enforcing the 2009 Health Breach Notification Rule and additionally stipulating that user data can't be sold for advertising purposes (Singer, 2023).

While the best way forward with this alternative would be comprehensive federal legislation, it is not very likely that Congress will come to a consensus soon because of partisan divides (Ng, 2023). After Roe was overturned last summer, Senator Warren introduced a bill that would prohibit the purchasing and transferring of sensitive geolocation data, which has unfortunately not advanced in the Senate (Marks, 2022).

Dignity: LOW Without comprehensive legislation, the dignity of Virginians citizens is still under serious threat. Current VCDPA legislation places the burden on Virginians to manage security risk. According to Lisa Druane of the ACLU: "[VCDPA] is based on opt-out consent. There are no civil-rights protections. There is no private right of action. A lot of the provisions are business-model affirming. It essentially allows big data-gathering companies to continue doing what they have been doing" (Klosowski, 2021).

Equity: LOW Similar to the previous criteria, the status quo leaves vulnerabilities open for users. People will still be prosecuted for digital records of seeking an abortion based on geolocation, text messages, and app data. This will disproportionately impact low-income users who rely on cell phones for the internet. No change to the current choice regime makes this policy LOW on the equity scale.

Political Feasibility: HIGH This intervention does not require any action by the Senator and thus does not require gaining support from her Republican colleagues. Since she faces no political opposition on this issue, this criterion is rated HIGH.

Administrative Feasibility: HIGH No change to the status quo will not require any investment of resources from the Senator or other parties. This criterion is rated HIGH for its administrative feasibility.

ALTERNATIVE 2: WASHINGTON STATE LEGISLATION

Out of all of the data privacy legislation currently passing through states, the most promising is HB 1155 “My Health, My Data” Act in Washington state. Unlike most data privacy legislation, it is focused solely on health oriented CGD. From the Attorney General’s press release, the bill:

- Prohibits organizations from selling Washingtonians’ health data.
- Blocks apps and websites — like health tracking apps, search engines and advertisers — from collecting and sharing Washingtonians’ health data without their consent.
- Prohibits “geofences” from being used at reproductive and gender affirming health care facilities.
- Requires companies that collect Washingtonians personal health data to maintain and publish a privacy policy for consumers’ health data. (Ferguson, 2022)

As of March 31st, 2023 the bill has passed the House and is in the Committee for Law & Justice in the Senate (Washington State Legislature, 2023)

Dignity: HIGH This intervention offers some of the strongest protections in state-level data privacy legislation. A large motivation for the policy was protecting Washingtonians’ dignity.

Equity: MEDIUM This intervention shifts the burden of responsibly from the consumer to the tech companies. Unlike current Virginia law, Data collection requires opt-in instead of opt-out consent.

Political Feasibility: MEDIUM-HIGH While text of the HB 1155 does not use the same "limiting powers of law enforcement" language that Senator Favola did, in the press release, it said the bill would “provide safe haven for individuals seeking care in our state." Otherwise, there is strong bipartisan support for this type of legislation.

Administrative Feasibility: MEDIUM Based on the fiscal impact statement of the Marsden 2021 data privacy bill, this would cost **$330,556** per year in personnel. According to the impact statement, the civil penalties would not cover the personnel costs (Department of Planning and Budget 2021 Fiscal Impact Statement, 2021).

ALTERNATIVE 3: ADVOCATE LEGISLATION

Last session, Senator Hashmi received two bills from an advocacy group for consideration to increase protections on reproductive health data. This legislation is unique from the rest of the bills because it is a package of two bills, one that concerns CGD and another that concerns PHI. The former is structured more like a data privacy bill whereas the latter expands on HIPAA regulations.

Each bill has two main purposes outlined. For the Non-PHI law, the Bill states:

> *This model bill prohibits the collection, retention, use, or disclosure of personal reproductive health data without the express, opt-in consent of the individual to whom the information relates and requires regulated entities to clearly inform individuals of the regulated entity's privacy policy regarding the collecting, retaining, using, and disclosing of personal reproductive health data. Further, the bill establishes an individual right to deletion of any such data and provides for enforcement through a private right of action and through agency enforcement.*

While the VCDPA does allow for users to delete their data, enforcing a private right of action goes above the current Virginia law. It also more specifically defines what "opt-in consent" looks like than the VCDPA (From the text: "clear and conspicuous, meaning is difficult to miss (i.e., easily noticeable). and easily understandable by ordinary consumers.")

The PHI centered bill mainly targets the court-order exceptions to patient consent when releasing PHI. If passed, this bill would prohibit law enforcement from issuing a warrant against those who may travel out of state for abortions. It borrows language from the 42 CFR part 2 of the Federal Code of Regulations, which prohibits data about substance use disorders from being released to law enforcement. Pulling text from the Federal Code adds legitimacy to this bill because it establishes precedent for this type of regulation. Unlike the Non-PHI bill, this bill has some carve outs for cases "showing a compelling need" to prosecute regardless of the law. The following analysis assumes the bills would be passed together.

ALTERNATIVE 3: ADVOCATE LEGISLATION

Dignity: HIGH This marks HIGH in the dignity criterion for the number of protections it affords users. One of the unique provisions of the bill is “data minimization,” which limits companies from obtaining data except when “absolutely necessary” to the operation of the business. This alternative ranks HIGH in the equity criterion because it places the highest standards of security by increasing restrictions on PHI and non-PHI data.

Equity: MEDIUM-HIGH It provides even greater equity than other alternatives because it promotes a private right of action, which allows citizens to go after companies that have misused their data and discourages companies from mishandling user data.

Political Feasibility: LOW This bill ranks LOW on the political feasibility criterion because of the two provisions concerning private right of action and prohibiting law enforcement collecting warrants on health data. As discussed in previous sections, both of these provisions have either stalled or killed potential legislation. Additionally, the language of the text primarily focuses on reproductive health data, which would raise alarms with opponents.

Administrative Feasibility: MEDIUM The costs for this are unknown, but may require new positions to manage policy and violations. It would also require coordination between the Virginia Department of Health and the Attorney General’s office for civil violations of data privacy legislation. It also may involve a new liaison position with industry knowledge who would need to communicate the statute to organizations that toe the line of coverage.

ADOPTION

The key to ensuring the recommendation's success is a careful and intentional adoption process. Before moving forward with this bill in the legislature, it would be advisable to meet with the sponsors of the Washington State Bill to learn about best practices, particularly with engaging stakeholder groups. Washington is home to many tech companies like Microsoft and Amazon, and they will undoubtedly have good advice on how to deal with these groups.

Then the Senator needs to engage with every community that might be impacted: the Medical Society of Virginia, lobbyists in the data privacy space, and tech companies (Google, Apple, Amazon, etc.). Tech companies need to be engaged with and informed early, otherwise narratives may get confused, which could lead to unnecessary political obstacles. Additionally, supporters in the reproductive rights space should be informed of the policy and adoption strategy in advance so they can offer behind the scenes support.

Other stakeholders in the legislature include the chairs of relevant committees, such as Appropriations in the House and Education & Health in the Senate. The chair has the responsibility of informing the caucus members about any bills or concerns with legislation. The chair also advises the leaders in both houses of what steps might need to be taken. In the state government, the Secretary of Health would be another good person to reach out to.

One potential opponent we haven't yet heard from are some organizations that have profited off of health data mining but have not been a presence in the legislature this year. For example, Weight Watchers has lobbied state legislatures for years to earmark money that is not for any real purpose. In Mississippi, the legislature spent $1.5 million to pay for subsidized Weight Watchers vouchers for teachers. Weight Watchers has faced a recent lawsuit from the FTC for illegally collecting sensitive health data of children in order to market apps to them. They may object to increased limitations on data collection.

It's ideal to bring the legislation to the Joint Commission on Health Care this spring to start to build support. For the Commission to put their official stamp of approval on the legislation, they must take a full committee vote. Their approval would bring a lot of political capital. However, if the vote ends in a non-endorsement, it will hurt the bill's chances of passing on the floor. Therefore, it may not be worthwhile to ask for their official endorsement, but a presentation could provide valuable feedback.

ADOPTION

To move this legislation, there are two different kinds of leadership the Senator could exercise: entrepreneurial organizing and shadow organizing.

Entrepreneurial organizing

The first method comes from Charles Cameron's Political Analyst Toolkit. According to his theory, issues with distributed benefits but concentrated costs require an entrepreneur to pass it. We can see this model clearly in this debate, since increasing protections helps all consumers, but a few tech companies will suffer. An entrepreneur can come in the form of a champion to carry it through within the legislature (like a Senator) or from outside (like an outside advocacy organization). It could also be created through a strong base, like approval from a voting block or commission. One notable example is Senator Favola, who recently gained a lot of national recognition from her failed bill in the legislature. She can draw on her new national networks to move this legislation. In another example of an entrepreneur, public criticism from Senator Elizabeth Warren pressured Google to stop tracking the locations of people who visited abortion clinics (Ng, 2022)

However, it is possible that attention could work against the Senator's goals. It is now commonplace for bipartisan issues to become politicized through the right wing media. With the wrong attention, conservative allies in the legislature may step back from supporting the bill. In my interview with Justin Sherman, he shared that there was Republican support for the bill he was working on with some Democratic colleagues in Congress. However, once the entrepreneurs connected the issue to abortion rights, the Republican colleagues backed out.

Shadow Organizing

Shadow organizing is working behind the scenes on an issue by framing the issue in a lens that attracts bipartisan support. This way, an advocate can build support from Republicans on what might seem like "liberal" issues. One of my colleagues has had an interesting problem with her client, a conservation advocacy organization trying to pass green legislation in West Virginia. She discovered that renewable legislation has been successful in red states when it has not been marketed as "green." Instead, conservative politicians lobby for these bills by promoting energy independence. The Senator may need to employ a similar type of tactic by focusing on speaking the language of her Republican colleagues more than trying to build national pressure.

ADOPTION

In shadow organizing, it's recommended to recruit Republican colleagues to lobby their colleagues. One potential ally I would recommend is Senator Todd Pillion, who represents the most southwestern district of Virginia. He is a pediatric dentist with a 100% Bill pass rate in the legislature. He is not at risk of losing his seat and won't make decisions based on re-election concerns. He also sits on the Senate Committee of Education and Health, one of the key committees the bill would pass through. His support could ensure it moves through committee without any problems. To bolster support in the house, Delegate Tran should also seek out a Republican ally who supports increased data privacy.

The worst case scenario is that the governor tries to politicize data privacy. It seems somewhat unlikely though, because this issue has not yet been picked up by national right wing extremist groups. If, however, this legislation is linked to abortion rights, the narrative could be co-opted, and the Senator may come under fire for a misinterpretation of the bill. This may be another reason why not to include Senator Favola.

Either way, implementation could be a big challenge in the event of politicization. The best path forward if it receives the wrong intention is to take this legislation off the docket until the media cycle moves past it. It may be even better to approach a Republican colleague and have them rewrite and sponsor the bill. Still, I am optimistic that the worst-case scenario will not be born out, and we will be able to enact this legislation soon.

IMPLEMENTATION

When session begins in January 2024, the Senator should introduce this legislation with her House colleague and co-sponsor, Delegate Tran. In addition to the legislation, they will need to submit a budget amendment to pay for personnel in the AG’s office to the appropriations committee. Once the amendment is passed, the legislation has been approved by relevant committees, and the Governor has signed it, the law will be implemented.

One additional provision of the legislation I would recommend is to include mandatory reporting by the AG’s office to the legislature. This is a common practice among other laws to check its progress and analyze if it’s necessary to revise the legislation. The Senator can request a report each Session from the AG's office to monitor the success of the bill.

CONCLUSION

This has been a difficult year for abortion rights. With the churn of negative stories, it is easy to lose hope. However, there are ways of protecting people wanting an abortion by creating more security around their personal data. Adopting the Washington State Health Data bill shows strong promise of creating protections for people seeking abortions. While the field is changing rapidly, this report has encapsulated nearly all available information about the subject to date. At the outset of this research, I was pessimistic about potential policy interventions. Now, I am cautiously optimistic.

APPENDIX I

DIGNITY AND EQUITY MEASUREMENTS

Dignity Calculation

Intervention	Consent Standards	Definition of CGD	Prohibition of geolocation of Health Care Facilities	Regulation on First and Third Party Practices	Total
Status Quo	1	0	0	1	2
Washington State Legislation	1	1	1	1	4
Advocate Legislation	1	1	1	1	4

Equity Calculation

Intervention	Informed Consent Standards	Opt In Consent for Data Collection	Private Right of Action	Anti-Discrimination Provision	Total
Status Quo	0	0	0	0	0
Washington State Legislation	1	1	0	0	2
Advocate Legislation	1	1	1	0	3

Appendix II

DESIRABLE LEGISLATIVE PROVISIONS

Below is a range of qualities a prospective legislation can have to protect consumers. Below is a list of best practices for laws. The ones in section 1: are strictly necessary, 2: preferable but not required, 3: desirable but not necessarily feasible.

Name	Description	Rationale
Consent Standards (1)	Regulated entities require users to "sign" a consent box before opting in. Consent standards would require regulated entities meet a certain standard of explaining policy (i.e. clear and comprehensible and not legalese).	Setting a standard that companies must conspicuously disclose practices to consumers increases transparency and accountability.
Definition of CGD (1)	CGD includes but is not limited to individual health conditions, geolocation near health care facilities, biometric health information, behavioral health data, and any consumer health data information that is derived or extrapolated from non-health information.	Regulated entities will exploit weak CGD definitions. This definition should be revised and revisited with emerging and changing trends.
Prohibition of geolocation of Health Care Facilities (1)	A more specific type of CGD. While most definitions of CGD will suffice, it must explicitly include any data related to the physical presence near health care facilities.	Geolocation of healthcare facilities can be used as evidence for prosecution by law enforcement or harassment by bad actors.
Regulation on First and Third Party Practices (1)	First and third parties are often regulated differently. Consistent regulating of both parties would involve grouping both as "regulated entities."	Different standards on parties create loopholes that are often exploited. Streamlining of practices ensures safety and accountability.
Anti-Discrimination Clause (1)	Prevents businesses from discriminating against users on the basis of race, sex, gender, religion,class or any other marginalized group.	This enables basic civil rights protections.
Data Minimization (2)	Typically refers to companies limiting collection of data altogether.	Not a necessary provision but help increase data security.
Data Security Standards (2)	Requires regulated entities to maintain specific security standards and outlines accountability in the event of a data breach. Legislative examples: NYSHIELD Act, Data Breach Notification Rule.	Increases user security; however, it is difficult to regulate the broad and differing data types. Requires additional consultation with experts to capture technical language.
Private Right of Action (3)	Policy that permits users to pursue legal action against companies who have violated terms of service.	Creates robust accountability mechanism, however, is extremely politically polarizing and hard to pass.

Works Cited

Brown, H. M., Bucher, T., Collins, C. E., & Rollo, M. E. (2019). A review of pregnancy iPhone apps assessing their quality, inclusion of behaviour change techniques, and nutrition information. Maternal & Child Nutrition, 15(3), e12768. https://doi.org/10.1111/mcn.12768

Citron, D. (2022). The Right For Privacy. W. W. Norton.

Danielle Citron [@daniellecitron]. (2023, February 22). Long thread on 230 arguments from yesterday. First Schnapper makes a total hash of the argument, failing to clarify how c1 and c2 work together, to emphasize what c1 was written to respond to, and to show how only immunity provision relates to taking blocking and filtering c2. [Tweet]. Twitter. https://twitter.com/daniellecitron/status/1628544432378109953

Department of Planning and Budget 2021 Fiscal Impact Statement (Fiscal Impact Statement Bill Number: SB1392). (2021). Virginia's Legislative Information System. https://lis.virginia.gov/cgi-bin/legp604.exe?211+oth+SB1392FES1122+PDF

Duhigg, C. (2012, February 16). How Companies Learn Your Secrets. The New York Times. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Elliott, V. (2022, June 7). Period and Fertility Apps Can Be Weaponized in a Post-Roe World | WIRED. Wired. https://www.wired.com/story/fertility-data-weaponized/

Equality and Human Rights Commission. (2018, May 25). Pregnancy and maternity discrimination research findings. https://www.equalityhumanrights.com/en/managing-pregnancy-and-maternity-workplace/pregnancy-and-maternity-discrimination-research-findings

Favola, B. (2022, December 29). SB 852 Search warrants; menstrual health data prohibited, definition. Virginia's Legislative Information System. https://lis.virginia.gov/cgi-bin/legp604.exe?231+sum+SB852

Feathers, T., & Fondrie-Teitler, S. (2022, October 20). Senator Questions Zuckerberg About Facebook's Collection of "Sensitive Health Information" – The Markup. https://themarkup.org/pixel-hunt/2022/10/20/senator-questions-zuckerberg-about-facebooks-collection-of-sensitive-health-information

Works Cited

Federal Trade Commission. (2021, June 22). FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others. Federal Trade Commission. 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

Ferguson, B. (2022, October 21). AG Ferguson, Rep. Slatter, Sen. Dhingra propose legislation to protect Washingtonians' health data | Washington State. Washington State Office of the Attorney General. https://www.atg.wa.gov/news/news-releases/ag-ferguson-rep-slatter-sen-dhingra-propose-legislation-protect-washingtonians

Frost & Sullivan. (2018, January 31). Femtech—Time for a Digital Revolution in the Women's Health Market. Frost & Sullivan. https://www.frost.com/frost-perspectives/femtechtime-digital-revolution-womens-health-market/

Gilman, M. E. (2021). Periods for Profit and the Rise of Menstrual Surveillance Are You There Law? It's Me, Menstruation. Columbia Journal of Gender and Law, 41(1), 100–113.

Gold, A. (2022, December 1). Tech warns Supreme Court ahead of landmark content cases. Axios. https://www.axios.com/2022/12/01/supreme-court-warning-tech-section-230-terrorism

Hackney, K. J., Daniels, S. R., Paustian-Underdahl, S. C., Perrewé, P. L., Mandeville, A., & Eaton, A. A. (2021). Examining the effects of perceived pregnancy discrimination on mother and baby health. Journal of Applied Psychology, 106, 774–783. https://doi.org/10.1037/apl0000788

Hart, C. E., & Zick, C. (2021, July 7). Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection. JD Supra. https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/

Hawkins, D. (2020, July 17). Analysis | The Cybersecurity 202: Why a privacy law like GDPR would be a tough sell in the U.S. Washington Post. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/

Klosowski, T. (2021, September 6). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Wirecutter: Reviews for the Real World. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Works Cited

Koepke, L., Weil, E., Janardan, U., Dada, T., & Yu, H. (2020, October 20). Mass Extraction. Upturn. https://upturn.org/work/mass-extraction/

Laidler, J. (2019, March 4). Harvard professor says surveillance capitalism is undermining democracy. Harvard Gazette. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

Ledford, C. J. W., Canzona, M. R., Cafferty, L. A., & Hodge, J. A. (2016). Mobile application as a prenatal education and engagement tool: A randomized controlled pilot. Patient Education and Counseling, 99(4), 578–582. https://doi.org/10.1016/j.pec.2015.11.006

Lina Khan [@linakhanFTC]. (2023, March 2). 1. Today @FTC took action to ban @BetterHelp from sharing people's data—Including sensitive mental health information—With Facebook and other companies for targeted advertising. Https://t.co/hP5LvqwPMH [Tweet]. Twitter. https://twitter.com/linakhanFTC/status/1631336092250132481

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. Washington University Law Review, 95(53).

Marks, J. (2022, June 17). Analysis | Anticipated Roe reversal brings a wave of data security reforms. Washington Post. https://www.washingtonpost.com/politics/2022/06/16/anticipated-roe-reversal-brings-wave-data-security-reforms/

Marsden, D. W. (2021, January 13). SB 1392 Consumer Data Protection Act; establishes a framework for controlling and processing personal data. Virginia's Legislative Information System. https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

McShane, J. (2023, February 19). Va. Republicans shelve bill to protect menstrual data from search warrants. NBC News. https://www.nbcnews.com/health/womens-health/va-republicans-shelve-bill-protect-menstrual-data-search-warrants-rcna71167
Mission. (2021, March 10). Federal Trade Commission. http://www.ftc.gov/about-ftc/mission

Works Cited

Moomaw, G. (2021, March 30). Virginia's new big tech-backed data privacy law is the nation's second. Critics say it doesn't go far enough. Virginia Mercury. https://www.virginiamercury.com/2021/03/30/virginias-new-big-tech-backed-data-privacy-law-is-the-nations-second-critics-say-it-doesnt-go-far-enough/

National Conference of State Legislatures. (2022, June 7). State Laws Related to Digital Privacy. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Ng, A. (2022, August 1). Data brokers resist pressure to stop collecting info on pregnant people. POLITICO. https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988

Ng, A. (2023, February 22). The raucous battle over Americans' online privacy is landing on states. POLITICO. https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775

Ollove, M. (2022, May 19). Some States Already Are Targeting Birth Control. https://pew.org/3lovVug

Paltrow, L. M., & Flavin, J. (2013). Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal Status and Public Health. Journal of Health Politics, Policy and Law, 38(2), 299–343. https://doi.org/10.1215/03616878-1966324

Reeves, R. V., & Venator, J. (2015, February 26). Sex, contraception, or abortion? Explaining class gaps in unintended childbearing. Brookings. https://www.brookings.edu/research/sex-contraception-or-abortion-explaining-class-gaps-in-unintended-childbearing/

Rosato, D. (2020, January 28). What Your Period Tracker App Knows About You. Consumer Reports. https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/

Sherman, J. (2023, March 6). GoodRx, Health Data Brokerage, and the Limits of HIPAA. Lawfare. https://www.lawfareblog.com/goodrx-health-data-brokerage-and-limits-hipaa

Works Cited

Sherman, J. (2023, March 24). Phone Interview with Justin Sherman [Personal communication].

Smith, M. (2021, June 9). ANALYSIS: Five Subtle Ambiguities in Virginia's New Privacy Law. https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-five-subtle-ambiguities-in-virginias-new-privacy-law

Solove, D. J., & Hartzog, W. (2013). The FTC and the New Common Law of Privacy. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2312913
Street, R. L., Gordon, H., & Haidet, P. (2007). Physicians' communication and perceptions of patients: Is it how they look, how they talk, or is it just the doctor? Social Science & Medicine, 65(3), 586–598. https://doi.org/10.1016/j.socscimed.2007.03.036

Vermont Laws, 9 V.S.A. § 2430. Retrieved November 3, 2022, from https://legislature.vermont.gov/statutes/section/09/062/02430
Vermont: Overview of the Data Broker Act. (n.d.). JD Supra. Retrieved November 3, 2022, from https://www.jdsupra.com/legalnews/vermont-overview-of-the-data-broker-act-6827402/

What Happens Now That Roe v. Wade Is Overturned? (2022, May 5). TheSkimm. https://www.theskimm.com/news/what-happens-if-the-supreme-court-overturns-roe-v-wade

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

Womack, J. J., Anderson, L. N., & Ledford, C. J. W. (2020). Presence of Complex and Potentially Conflicting Information in Prenatal Mobile Apps. Health Promotion Practice, 21(2), 238–245. https://doi.org/10.1177/1524839918796216

Zakrzewski, C., Verma, P., & Parker, C. (2022, July 6). Texts, web searches about abortion have been used to prosecute women. Washington Post. https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/