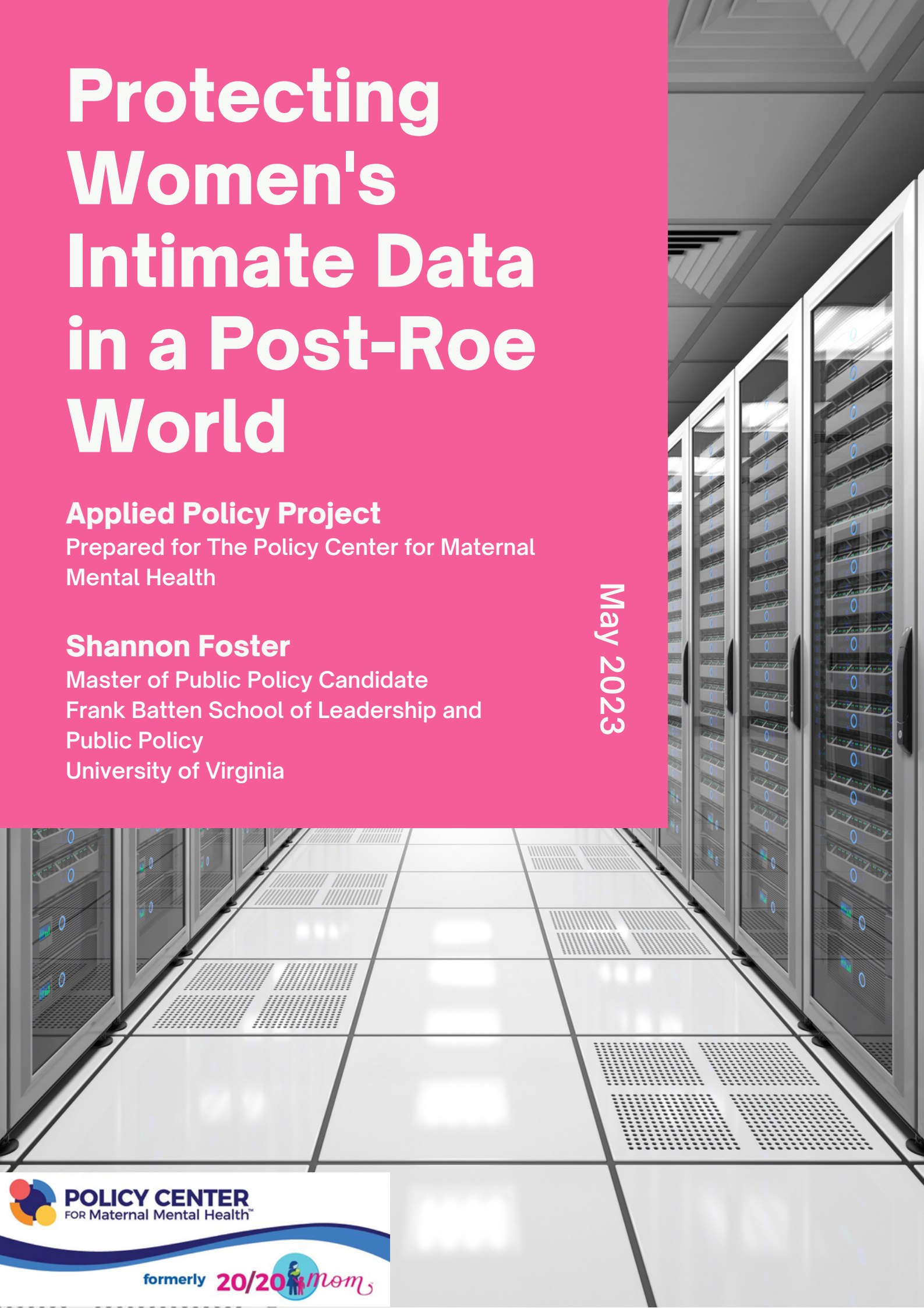
Protecting Women's Intimate Data in a Post-Roe World

Applied Policy Project
Prepared for The Policy Center for Maternal Mental Health

May 2023

Shannon Foster
Master of Public Policy Candidate
Frank Batten School of Leadership and Public Policy
University of Virginia



POLICY CENTER FOR Maternal Mental Health™
formerly 20/20 mom

Acknowledgements

I would like to thank The Policy Center for Maternal Mental Health, specifically, their fabulous program manager, Sarah Johanek, for affording me the opportunity to conduct a meaningful policy analysis and pursue my interests protecting vulnerable women. I'd also like to thank the Center's Founder, Joy Burkhard, for her support and leadership in this fight.

Thank you to all of my spectacular professors at the Frank Batten School of Leadership and Public Policy for preparing me with the knowledge and tools necessary to undertake this project. I would like to thank my first APP instructor, Noah Myung for arming me with his honest feedback. A very special thanks to Professor Volden for his support navigating the nuance of the national policy process.

Thank you Professor Warburg for connecting me with the feminists who translated my aspirations for women's rights into a profession. Thank you Professor Turner for your kind words of encouragement; thank you Professor Stewart for giving me the voice to speak; and thank you Professor Adams for spurring my affinity for seeing policy through the lens of psychology and mental health.

I am eternally grateful to my APP partners from both semesters--Alex Frazier, Abby Rothenberg, Priya Viswanathan, and Liz Nigro-- for motivating me to overcome challenges and providing instrumental feedback. Thank you Allison, Andrea, Victoria, and Noah for your laughter and support.

Finally, I would be remiss without thanking my family. Thank you Mom, Jessie, Alex, and Jacob for believing in me while I floundered forward. Thank you, Dad, for being my eternal sounding board and for offering your uncannily encyclopedic knowledge at all hours. Thank you to Ian for whipping up pancakes while I edited the following work.

Client Profile

The Policy Center for Maternal Mental Health, formerly known as 2020 Mom, is a 501(c)3 non-profit committed to ensuring “all pregnant and postpartum mothers have ready access to standardized, evidence-based maternal mental health care from providers they respect and trust” (Burkhard, 2023). TPCMMH engages with community stakeholders as well as with corporate and philanthropic actors through informational programs and grassroots advocacy.

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 Pledge

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

Table of Contents

Acronyms & Definitions

- **ADPPA**: American Data Privacy and Protection Act
- **ANPR**: Advanced Notice of Proposed Rulemaking
- **CFPB**: Consumer Financial Protection Bureau
- **CPs**: Compliance Personnel
- **CRS**: Congressional Research Service
- **DBL**: Data Broker Law
- **DPBR**: Data Privacy Bill of Rights
- **EFF**: Electronic Frontier Foundation
- **FTC**: Federal Trade Commission
- **ITIF**: Information Technology & Innovation Foundation
- **PRA**: Private Right to Action
- **TPCMMH**: The Policy Center for Maternal Mental Health, formerly known as 2020 Mom
- **UDAAPS**: Unfair, deceptive, or abusive acts or practices committed by those who offer products or services to consumers.

Executive Summary

The current data privacy environment is rapidly changing in America. New, innovative technologies represent a boon to the economy, yet a bust to consumer protections. The protection of personal information has always been essential to user confidence, but the overturn of *Roe v. Wade* has rendered women in trigger law states especially vulnerable to the exploits of data brokers and the intrusion of law enforcement. The *Dobbs v. Jackson* decision unraveled privacies protected by HIPAA, allowing data brokers to profitably expose information previously regarded as confidential between a woman and her provider. The decision is changing reproductive healthcare and jeopardizing women's mental health in the process.

If we fail to protect women's sensitive data, 1 in 3 American women of child-bearing age face legal exposure from information sold by data brokers to law enforcement ("U.S. Census Populations with Bridged Race Categories," 2022).

The following three options are designed to reduce data vulnerability, empower women to control their online presence, and prevent exposing sensitive information.

Alternative 1: CRS Report of The Fourth Amendment is Not For Sale Act (S.1265)

Alternative 2: Emergency FTC Funding

Alternative 3: Propose a Data Privacy Bill of Rights, with or without the Private Right to Action

After assessing the impact each alternative on the legal exposure and online empowerment of women in trigger law states, I recommend Alternative 1 and Alternative 3 in tandem. This combination is the most effective, politically feasible, and equitable option, with manageable costs.

This report concludes with guidance on implementation, including what can be done if Congressional action is stalled for national security reasons, if the original coalition of lawmaking actors are distracted by other matters, or those legislators lose their seats.

Problem Statement

Following the *Dobbs v. Jackson* decision overturning the right to abortion, prosecutors now use intimate health information from online sources and apps to determine if women in “trigger law” states accessed newly unlawful reproductive care. If we fail to protect women’s sensitive data, 1 in 3 American women of child-bearing age face legal exposure from information sold by data brokers to law enforcement (“U.S. Census Populations with Bridged Race Categories,” 2022).

Background

The State of Data

When users surf the internet, they leave behind digital bread crumbs that are collected, aggregated, and sold to the highest bidders. These are called “first-party cookies.” They are text files and small bits of data used to identify specific users within a computer network (U.S. Department of Homeland Security, 2014). The cookie evolved to include “third party cookies,” where companies plant code in a user’s browser allowing them to track where else they go on the internet. “Persistent cookies” are stored on a browser after users exit the tab. Although they expire on a set date, most users neither know how long they remain on browsers nor know how to remove them (“What Are Cookies?,” 2018).

Six in ten American adults say they do not think it is possible to go through daily life without having data collected about them (Auxier et al., 2019). The presence of cookies is often justified by 'improvements to experience' of personalized advertising based on recent internet history. However, sites that ask users to accept their cookie policy often offer a secondary option to 'adjust cookies settings.' Although some sites do allow users to prevent tracking, the adjustment option often leads down a rabbit hole of company legalese and jargon the average user is unlikely to understand. If one opts to refuse cookies, their experience might worsen as features stop working as intended and processing power is compromised. Even if users opt-out, many browsers automatically accept cookies, including Chrome, Firefox, Safari, and Microsoft Edge (Chen, 2021).

Given the strikingly specific location-based advertisements which pop onto app interfaces, users are growing increasingly aware of the precision with which apps track them. Apps such as the ‘family tracking app’ Life360–which allows parents to monitor their children’s speed while driving– have been found to sell over 33 million users' geolocation data to over a dozen different brokers (Keegan and Ng, 2021). Companies like Life360 claim they de-identify information, scrambling personal identifiers tracking information back to individuals. However, researchers found that 99.98% of Americans could be correctly re-identified in any dataset using a mere 15 demographic attributes (Rocher et al., 2019).

"Researchers found that 99.98% of Americans could be correctly re-identified in any dataset using 15 demographic attributes."

The many hands who use and pass off data to others are not obvious to most consumers. The three main parties in the sale of data are the subject (the person to whom the information relates), the controllers (the responsible party who determines why and how to process the information), and the operator (a person who processes personal information on behalf of the responsible party, such as a data broker or IT vendor) (Michalsons, 2015).

Data brokers take raw data and pull out insights that are important to drive smart business decisions. Data analytics reduce business costs and develop new and innovative products and services. More specifically, it's used to (1) predict future sales or purchasing behaviors; (2) to analyze the effectiveness of marketing; (3) to boost customer acquisition and retention; (4) or to accelerate supply chain efficiency (Hillier, 2022).

Services use device identifiers that allow brokers to harvest information from a device across apps by matching tracker IDs held in company databases. These identifiers are then used to "determine whether our marketing is successful" as The New York Times's own cookie policy describes. Companies like TowerData buy up those tracking identifiers and sell them to apps and companies to help brands identify who is using their product (Oliver, 2022).

These "Client IDs" amass myriad data points about individuals that are aggregated into groups. Experian, one of the major American data brokers, has group names called "Couples with Clout," "Ambitious Singles," "Boomers and Boomerangs," "Golf Carts and Gourmets," and "Kids and Cabernet" (Ikemura, 2010). These lists can be sold to any individual, company, or organization that can afford them, most frequently to advertise to groups likely to complete a purchase (Oliver, 2022).

More intrusive groupings can include sexual preferences or ailments like high blood pressure or cancer, such as "Suffering Seniors," "Pay Day Loan Central-Hispanic," and "Help Needed–I Am 90 Days Behind with Bills" (Oliver, 2022). Much of this information is, in a medical situation, protected under the Health Insurance Portability and Accountability Act (HIPAA) (Office for Civil Rights, 2009). However, one researcher found that "if you go to a medical website and search for 'HIV' or 'abortion,' that information is not protected at all" (Coutts, 2018). This raises serious concerns about the protection of online identities and intimate information.

Biometric Data and Reproductive Access

These groupings frequently aggregate biometric data. According to the Biometrics are unique physical characteristics that may be used for automated recognition. They can include biological indicators, such as fingerprints, facial features, or veins, or data scrubbed about physical characteristics and health (Botezatu, 2018). The main difference between biometric data collected via cookies and app-specific data is that app information is voluntarily input by users.

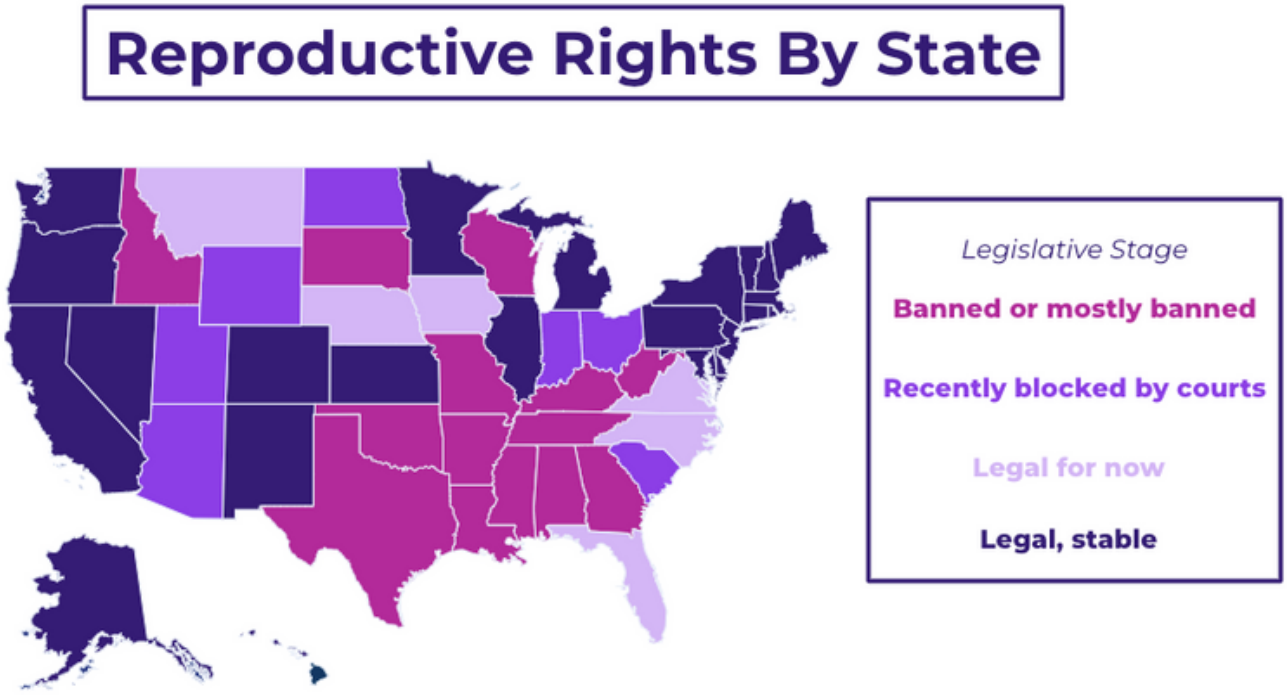


Figure 1: U.S. Reproductive Rights by State (Source: The Guttmacher Institute)

In 2022, Nebraska police accessed private Facebook messages and user data of a mother whose daughter allegedly sought and used abortion pills. The police compiled not only the mother's private messages, but also extensive user information, profile contact data, and user IDs directly from Facebook (Koebler & Merlan, 2022). Later that year, the FTC released an Advanced Notice of Proposed Rulemaking (ANPR) to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Question 5 asks if commercial surveillance practices or lax security measures lead to harms that consumers may not immediately identify. Some comments mention the less-easily identifiable harms derived from fears about how personal data can be used to prosecute those seeking abortions. This prompts consumers to stop using tools and apps designed to improve self-monitoring of healthcare. One comment argues it is wrong to allow people to live in "constant fear and anxiety, and this phenomenon has the potential to lead to severe injury, illness, and death, as people attempt to protect their data by cutting corners in their own healthcare" (RE, 2022).

Post *Dobbs v. Jackson*, states can render reproductive services inaccessible and illegal, and experts warn that prosecutors can now use data evidence like search engine histories, phone records, text messages, geolocation data, social media activity, and personal health records to construct cases against those who illegally seek such healthcare. Emma Roth, a staff attorney with National Advocates for Pregnant Women, warns that "these mass surveillance tools have the potential to sweep hundreds or thousands of people within their ambit and subject them to potential investigation and prosecution" (Ali, 2022). Many downstream risks are yet unknown. Given the widely unregulated commercial space, tech companies who gather data hesitate to clarify their procedures related to relinquishing data to law enforcement (McGill & Fried, 2022).

Period-tracking apps like Flo and Clue are a major cause for concern since the *Dobbs* decision. These apps track intimate information like the start and end dates of user periods and pregnancies. This deeply personal data can be sold or given to law enforcement at no or low cost to determine if someone has or is considering an abortion. The FTC recently reached a settlement with Flo Health Inc. after a 2019 Wall Street Journal investigation found the app disclosed menstruation and pregnancy data of millions of users to third parties, including Google and Facebook, without limiting how the third parties could use the information (Torchinsky, 2022). The 2021 settlement required Flo Health Inc. to obtain the affirmative consent of users before sharing their personal health information and to obtain an independent review of their privacy practices, but its exceptions for law enforcement are unclear. There is nothing to stop these apps from sharing this info with prosecutors (FTC Finalizes Order, 2021; Baumann, 2022).

Location data about people visiting clinics can also be collected and used against those seeking vital healthcare. This information can be gathered via seemingly banal apps. Earlier this year, a location data firm called SafeGraph was found selling information about patients visiting clinics that provide abortions, having obtained location data from weather and prayer apps (Torchinsky, 2022). The Electronic Frontier Foundation (EFF) has argued that period tracking apps pose a pressing danger for women seeking reproductive healthcare (Gebhart & Barnett, 2022). In response, Google announced it will automatically delete geolocation data of users who visit medical facilities (Morrison, 2022). Similarly, the period tracker app Flo debuted an "anonymous mode" to empower users to delete identifiable information from their accounts (Thibault, 2022).

The EFF contends the most common scenario whereby a woman is criminalized for her pregnancy outcomes is when a third party turns them into law enforcement, such as hospital staff or a family member. However, the most common forms of evidence used in resulting investigations are those texts, emails, or information gleaned from apps or cookies (Gebhart & Barnett, 2022).

Literature Review

The Public Is Calling: Will Lawmakers Listen?

One 2019 study from the Pew Research Center finds only one-third of adults say they understand current data protection laws and four in five say they aren't confident that companies will admit to misuse of their personal data. Seventy-five percent of adults say there should be more government oversight over data usage (Auxier, 2020). This is backed by the Nonpartisan and Objective Research Organization Center (NORC) for Public Affairs Research which found that nearly three-quarters of Americans want the federal government to establish national data privacy standards (Sterrett, 2022).

What is causing the disconnect between public demand for privacy and privacy regulation? Many experts point to the data brokers profiting off users' inability to comb through privacy agreements hundreds or thousands of pages long. They often say that by making the user the commodity instead of having them pay for the product, they can keep the price point low or even free (Oliver, 2022). They argue it improves the product by ensuring that advertisements are personalized, making ads more relevant for consumers and more beneficial for companies (Bertini & Wathieu, 2010). This neglects the widespread violations of consumer trust stemming from "personalization."

The following sections discuss related federal and state laws proposed or passed in the United States, as well as one notable European bill that is the most comprehensive data privacy bill ever passed. However, given how unexpectedly *Roe v. Wade* decision was released stateside, none of these laws were designed with women's intimidate data in mind. Instead, they were intended to defend information gleaned for commercial purposes.

State Privacy Regulation: A Patchwork Project

Experts also point to the patchwork of laws enacted at the state level that feature varying degrees of user protection. Although some oversight is certainly preferable to none, national regulators defer to state legislatures, arguing they are more in-touch with their constituencies and are therefore better equipped to regulate their markets. State legislatures across the country have paved their own ways to data privacy. Most notably, California was among the first to pass a comprehensive privacy measure, the California Consumer Privacy Act ("California Consumer Privacy Act (CCPA)," 2018). The landmark law protects the right to know about how personal information is collected and shared (§D. Required Notices), the right to delete personal information (§E. Requests to Delete Personal Information), and the right to opt-out of the sale of their personal information (§B. Requests Not to Sell Personal Information) (Friel & McLellan, 2019). The CCPA is enforced in civil penalties via the California attorney general.

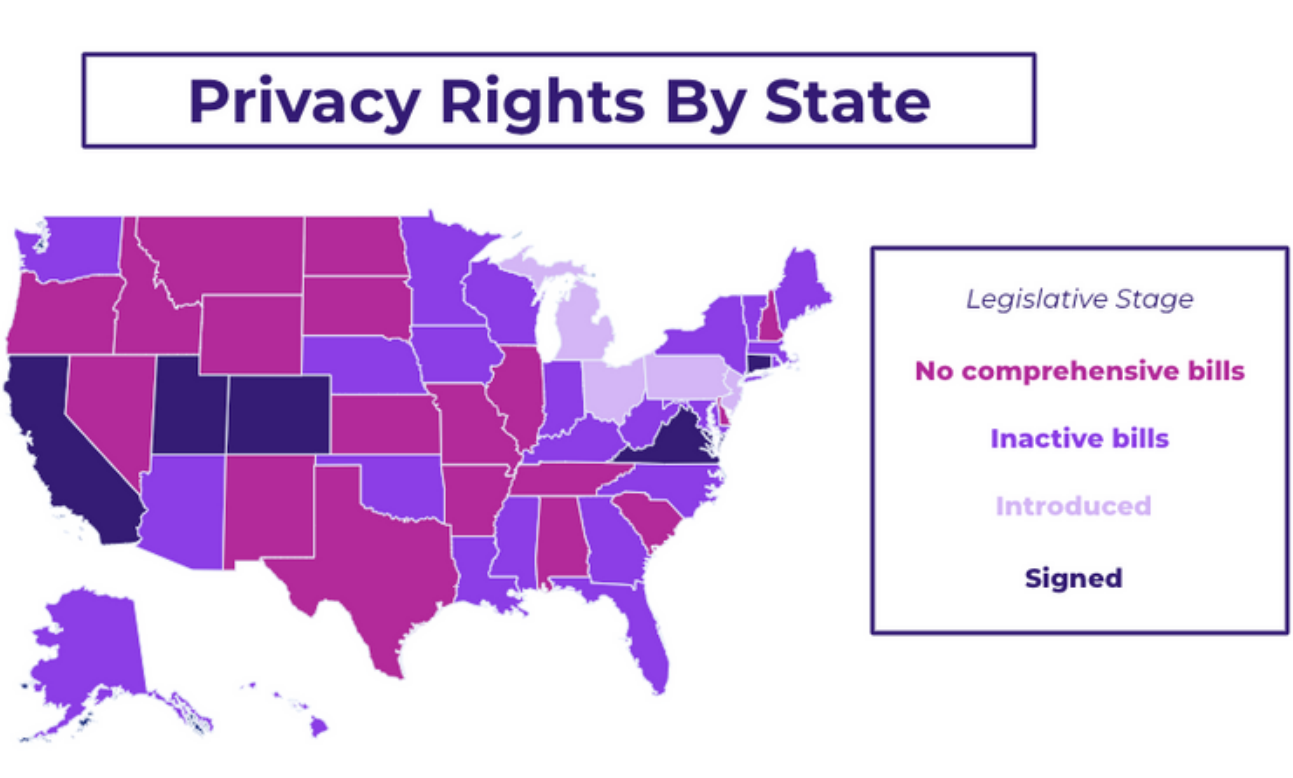


Figure 2: U.S. Data Privacy Laws by State (Source: The Westin Research Center)

One month after the CCPA passed, Vermont shepherded its Data Broker Law, which defined a data broker as "an individual or business that collects and sells or licenses the brokered personal data of a consumer, even if there is no direct business relationship" ("Guidance on Vermont's Act 171 of 2018 Data Broker Regulation," 2018). The DBL included an annual registration requirement for brokers.

At least 31 other states have enacted heightened security requirements to usher in a new era of consumer data protection. Figure 2 demonstrates the many stages where states sit in pushing for greater privacy protections (Cosgrove, Lively, Adams, Wang, & Fazlioglu, 2023).

This approach led to a patchwork system whereby states must individually confront inconsistencies in interstate requirements. As a result, America is beginning to observe the patchwork's impact on the American economy including innovative repercussions in the tech market; disproportionate difficulties imposed on small business and startups; issues regarding accessibility for consumers and companies; deteriorating long-term consumer confidence; complex implementation across states; and regulator resource strain (Castro, Dascoli, & Diebold, 2022).

Challenges to Federal Data Legislation

Congress may seek to adopt a comprehensive system for data protection by expressly preempting state laws. Several attempts at data privacy, such as the American Data Privacy and Protection Act, have left states with strict data protections out of the equation, including California's Consumer Privacy Act ("California Consumer Privacy Act (CCPA)," 2018), Illinois' Personal Information Protection Act– which imposes requirements on covered entities that collect, handle, or store non-public personal information ("Personal Information Protection Act.," 2013)– and Illinois' Protecting Household Privacy Act–which prohibits law enforcement from obtaining household electronic data without a warrant barring consent or emergencies (Kabaria & Seiver, 2022).

Data privacy bills introduced to Congress are first referred to the House Committee on Energy and Commerce and the Subcommittee on Consumer Protection and Commerce. Such bills are often referred to the Science, Space and Technology Committee as well as the Homeland Security Committee as well. Although protecting user data from bad actors is an important security concern, this last committee and its purview are outside the scope of this project.

The House Committee on Energy and Commerce Chairwoman, Cathy McMorris Rogers (R-OR), recently delivered the opening remarks at the markup session for the American Data Privacy and Protection Act earlier calling for citizens to have "more control over their information online" (Rodgers, 2022). Ranking Member Frank Pallone (D-NJ) and McMorris Rogers released a joint press statement hailing the ADPPA for its core rights protections (Hendrix, 2022). The ADPPA was favorably viewed by the Subcommittee on Consumer Protection and Commerce since the passage of a remarkably similar bill– the American Competitiveness Of a More Productive Emerging Tech Economy (American COMPETE) Act– that directed the FTC to study and report on targeted advertisements. These factors indicate fertile ground for bipartisan lawmaking (Hendrix, 2022).

Chairwoman Maria Cantwell (D-WA) proposed her own privacy bill in 2019, the Consumer Online Privacy Rights Act (COPRA). She is both a knowledgeable proponent of data protections as well as a potential obstacle in the event that further bills do not closely resemble COPRA priorities, such as a short phase-in period for the private right to action (PRA). Senator Jerry Moran (R-Kan.), who is on the Senate Subcommittee on Consumer Protection, Product Safety and Data Security, released his own Consumer Data Privacy and Security Act in 2021. Although it failed, it corralled Republicans on the committee into supporting preempting state laws. However, Moran's bill did not include any provision that would allow individuals to sue companies over privacy violations– a sticking point in negotiations.

Enforcement would primarily be spearheaded by the FTC, having already brought forth hundreds of enforcement actions, most of which resulted in companies entering into consent decrees to prevent any further violations. While these consent decrees are not legally binding, they are significant given their reflection of the practices the FTC views as "unfair" or "deceptive" (Cohen, 2022). However, the FTC cannot seek monetary penalties for first-time UDAAP violations. It can only seek cease-and-desist orders or settlement agreements, and they lack jurisdiction over financial institutions, non-profits, and common carriers (Cohen, 2022).

Many businesses operate across state lines and industries, making adherence to distinct, location-specific standards costly. Federal legislation would help avoid burdensome reporting and compliance costs and update now-antiquated state laws (Castro, Dascoli, & Diebold, 2022). Many older laws are obsolete given the pace of technological advancement, although many provide the foundation for new regulatory coalitions. These laws differ in scope, enforcement, and penalties:

- Communications Act (1934): Provides data protection provisions for common carriers, cable operators and satellite carriers.
- Fair Credit Reporting Act (1970): Covers the collection and use of data in consumer reporting agency files to promote accuracy, fairness, and privacy.
- Electronic Communications Privacy Act (1986): Prohibits unauthorized interception of electronic communications (e.g., wiretapping).
- Health Insurance Portability and Accountability Act (1996): Requires national standards to protect sensitive patient health information.
- Gramm-Leach-Bliley Act (1999): Requires financial institutions to explain their information-sharing practices to customers.
- Children's Online Privacy Protection Act (2000): Protects the online data of children younger than 13 years old.
- Consumer Financial Protection Act (2010): Regulates unfair, deceptive, and abusive practices (UDAAPS) related to financial products or services.

The 1974 U.S. Privacy Act established "a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals…in systems of records by federal agencies" ("Overview of the Privacy Act of 1974" 2020). Twenty-two years later, the Health Insurance Portability and Accountability Act (HIPAA) regulated privacy in the healthcare industry, and three years later, the Gramm-Leach-Bliley Act protected private information in the financial industry. The 2000 Children's Online Privacy Protection Act (COPPA) prohibits websites from asking for personal information from children under the age of 13 without parental consent (Federal Trade Commission).

Still, Congress better resembles a privacy graveyard than an adaptive policy machine. Previous laws regulate a technical mise en scène which no longer exists. Bipartisan efforts to push privacy provisions have fallen flat in both Houses. For example, Florida Senator Marco Rubio's American Data Dissemination Act of 2019 unsuccessfully attempted to "impose privacy requirements on providers of internet services similar to requirements imposed...under the Privacy Act of 1974" (Rubio, 2019). In October of 2022, Democratic Representative Frank Pallone Jr. (NJ-06) sponsored the American Data Privacy and Protection Act, a bill Democratic staffers admit is more designed to socialize American conversations about the sale of vulnerable data than be signed into law (H.R.8152, 2022).

The EU's Unprecedented Right to Privacy

The General Data Protection Regulation (GDPR) addresses data protection and privacy in the European Union and throughout the European Economic Area. It is enforced by the Information Commissioner's Office, the UK's "independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals" ("Upholding Information Rights for All a Guide to the Legislation the ICO Regulates," 2012). Passed in 2016 with a 2018 compliance date, the GDPR is a cornerstone of EU privacy and human rights law ("European Union - Data Privacy and Protection," n.d.).

The GDPR was designed to empower user control over personal data and to streamline the legislative environment for businesses (van Ooijen & Vrabec, 2018).

The GDPR was developed with seven principals in mind:

1) Lawfulness, fairness and transparency;
2) Purpose limitation;
3) Data minimization;
4) Accuracy;
5) Storage limitation;
6) Integrity and confidentiality (security); and
7) Accountability ("The Principles," 2019).

These seven components emphasize disclosing how personal data is collected and processed; revealing companies' minimum amount of personal data needed to fulfill their purpose; requiring inaccurate data be quickly redressed; retaining data with individually-linked identifiers no longer than is necessary; and regularly demonstrating compliance (Information Commissioners Office, n.d.).

Perspectives on the long-term impacts of the GDPR vary widely. Proponents say the GDPR has pushed data privacy to the forefront of global conversations. As of this year, more than 100 countries have put new privacy standards in place, including Brazil, Chile, Japan, South Korea, Argentina, and Kenya (Jones, 2021). For example, Canada added a Digital Charter to their Personal Information Processing and Electronic Documents Act (PIPEDA). It addresses cookies and opt-out protocols (Jones, 2021). Even Australia's 1988 Privacy Act was updated in 2021 to be aligned with GDPR regulations (Christie, 2020).

However, three year's worth of research following the GDPR's publication has revealed setbacks as companies and investors attempt to comply with its requirements. Critics contend that the GDPR negatively affects the EU economy and stifles innovation. One 2018 study found that over half of 500 mergers and acquisitions in Europe, Africa, and the Middle East experienced delayed transactions due to compliance concerns (Carraro, 2018). Bitkom–Germany's digital trade association representing over 2,700 companies–found three in four respondents said the GDPR was the primary obstacle to innovation. This is an 11 percentage point jump from the previous year and a 29 percentage point jump from 2017 (Streim & Weiß, 2019).

Other studies found that 40% of U.S. firms with a data presence in the EU have spent an average of $10.1 million in compliance efforts following 2016, indicating that the regulation drains company resources (Chivot & Castro, 2019). On the other hand, it also suggests that more closely aligning U.S. regulations with the GDPR's central principles could reduce inefficiencies in complying with both markets. Regulatory alignment could present a cost-saving measure for American companies.

Other research finds the GDPR hurts European tech startups, causing a decline in investments for new ventures and a loss of around 30,000 jobs (Jia, Jin, & Wagman, 2018). However, this evidence may not demonstrate a causal relationship between the GDPR and economic setbacks. That same study attempts to attribute the GDPR with a decrease in the number of monthly deals for new EU ventures: an €8 million ($8.1 million) dip in monthly amounts invested in the healthcare sector per member state and a €7 million ($7.08 million) dip in financial sector investments. Due to the dynamic, multidimensional nature of each of these markets and the many factors impacting new businesses, it's unlikely the GDPR can be held solely responsible. During a period in which the EU adopted over 1,000 acts, hundreds of which directly pertain to the health and financial sectors ("Legal Acts – Statistics," 2023), a causal relationship is unlikely.

Only days after the 2018 GDPR enforcement deadline passed, comparable legislation was drafted stateside. Virginia's senior Democratic Senator Mark Warner developed a list of policy options for national legislation he dubbed a "comprehensive GDPR-like data protection legislation" (Warner, 2018). The provisions are broken down into three categories:

1. Mirroring GDPR features such as:
    a. Data portability: individuals obtaining their data for private purposes;
    b. The right to be forgotten, which is the user's right to force covered entities to clear records of past engagement; and
    c. First party consent, or the ability to record calls or online conversation so long as you are a party to the conversation.

2) Handling personal data in systems built with privacy by design and default, whereby privacy procedures are integrated into technology upon creation.

3) Pseudonymisation or full anonymization, meaning the de-identification by which personally identifiable information data are replaced by artificial identifiers (The European Parliament And The Council Of The European Union, 2016).

Connections to Post-*Roe* Privacy

Overall, there is a dearth of literature that assesses the impact of these state and federal laws–proposed or passed–on the exposure of women's intimate data privacy post-*Roe*. This can be attributed to how recently and unexpectedly the reversal of the right to an abortion occurred. Most social scientists and journalists were blindsided by the leak revealing the Court's likely decision. As a result, the research community was woefully underprepared for the potential vulnerability of women's fertility data, failing to consider the possibility that their privacy efforts–or lack thereof–could be applied to this particular realm of online information.

In an ideal world, researchers would formally study the impact of various data protection mechanisms, such as the following sections' legislative and regulatory vehicles. Although such studies do not yet exist, the rest of this report is dedicated to determining what options are most effective at reducing legal exposure, increasing digital autonomy, and improving comfort using online services, as well as evaluating which options are the most politically feasible and the most equitable at the lowest cost.

Evaluative Criteria

This report will prioritize the following evaluative criteria: effectiveness, feasibility, equity, and cost. Effectiveness and equity were chosen to ensure alternatives further TPCMMH's objectives, while feasibility ensures alternatives can reasonably be implemented given the political and regulatory landscape in which they operate. Cost is a necessary component to address potential pushback from the business community.

EFFECTIVENESS

Effectiveness, as defined by TPCMMH, is optimizing women's welfare.
This report seeks to answer the following questions:

- Will this option make women feel comfortable utilizing online services to monitor their health without fear of legal retribution?
- Will this option reduce the number of women whose sensitive data is available for resale by data brokers to law enforcement?
- Will this option increase women's autonomy over who accesses their information?

For each alternative, we will assess the immediacy of impact, noting any delays in efficacy and anticipating substantial political or implementation barriers.

POLITICAL FEASIBILITY

TPCMMH defines political feasibility as an appeal to both the business and women's welfare camps. Findings will be rated 'highly feasible' (high), 'likely feasible' (medium), and 'somewhat feasible' (low) according to (1) a favorable stakeholder analysis, (2) policy sustainability, and (3) administrative robustness. Alternatives that satisfy all three criteria will be considered politically feasible:

- **A stakeholder analysis** determines the alternative's strength and the resources available to the opposition versus support coalitions. The analysis will consist of web searches, online interviews with relevant actors such as elected (Congresspeople and their staffs) and appointed (FTC and staff) officials, victims of data privacy violations (from articles, op-eds, and NPRM comments), trade associations, professional societies, advocacy groups, ideological coalitions, and data brokers.

- **Policy sustainability**, in the event of successful implementation, refers to a solution's durability in improving the protection of female users of apps and services alongside the solution's likelihood of judicial survival. Sustainable policy will outlast its enacting coalition, maintain its integrity, and stave off unwarranted political pressures through bipartisanship and coalition-building (David Leo Weimer & Vining, 2017, pp. 280–303). Alternatives will be evaluated on a spectrum from immediate deployment and immediate impact to delayed impact yet prolonged expected benefits, as well as sensitivity to shifts in Congressional balances of power.

- **Administrative robustness** addresses the possibility of failure in implementation, taking into account bureaucratic incentives, preferences, capacities and targets. This will depend upon the specificity of the bill or legislative vehicle's language to assess its level of ambiguity and built-in bureaucratic discretion.

EQUITY

Alternatives must ensure benefits are distributed equally across women. To ensure the protection or access to compensation isn't regressive (imposing a larger relative burden on low-income women), this report will examine the 'hassle factor' of accessing benefits. We will prominently feature the potential for distinct impacts on different subpopulations, including those whose primary language is not English, and individuals of different ages, technological savvy, and familiarity with government systems.

COSTS AND BENEFITS

This criterion will weigh the maximization of women's welfare against the financial impact on businesses. Given that several alternatives do not solely affect the target population--women in trigger law states-- this report better suits a holistic analysis as opposed to a traditional cost-benefit analysis.

This report examines the value to women in trigger laws as those who stand to benefit and those who otherwise would not have had the option to pursue retribution or manage their online presence. This will broadly be compared to the costs to lawmakers. and regulatory bodies, as well as those endured by businesses. Such analysis weighs the wealth created through action, diseconomies from up-front, back-end, and ongoing compliance costs, alongside adverse effects on investment and bankruptcy.

Results will color our understanding of which actions will have the greatest impact on women's legal vulnerabilities compared to its associated costs.

Alternative 1: CRS Report Request

The Fourth Amendment was intended to shield against unreasonable searches and seizures of physical property, such as one's home or personal correspondence. However, contemporary Fourth Amendment doctrine has expanded beyond its property-based origins to include a broader, unenumerated right to privacy which evolved in response to new surveillance technologies, including wiretapping and thermal imaging (Gu, 2022). Such protections are necessary to defend against technologies that the Framers could never have anticipated. However, the current Court's textual interpretations may result in the crumbling of Fourth Amendment protections against modern surveillance.

The CRS is yet to issue a report covering The Fourth Amendment Is Not For Sale Act (H.R. 2738/S. 1265). Proposed in 2021 by Ron Wyden (D-OR) and Rand Paul (R-KY), the bill requires government actors obtain a court order to compel data brokers to disclose data. Although it never made it to the floor, 2022's Meta and Flo privacy invasions and renewed privacy coalition support suggest a CRS report revisiting HR. 2738--and the renewed anti-intrusion effort that would follow-- may be an effective vehicle to protect women in "trigger law" states ("Coalition Calls for Congressional Hearings on the Fourth Amendment Is Not for Sale Act," 2021).

This option requires arranging a call with a Sen. Wyden staffer discussing the request; orchestrating an informal conversation between that staffer and a CRS official to negotiate timing and research capacity; that Sen Wyden's office draft a formal letter requesting a report about the bill's relevance in 2023; and the acceptance and completion of the report. This may require renewed support from coalition leaders and new allies in the women's health arenas. TPCMMH must prepare that coalition quickly following the report to draft an updated version of H.R. 2738.

EFFECTIVENESS

S.1265 would close the existing legal loophole which enables FBI and state/local law enforcement to purchase citizens' intimate online information from data brokers without a warrant. This bill would necessitate government entities obtain court orders before compelling data brokers to disclose user data, meaning they could no longer purchase Facebook information, Google search histories, or biometric app data from brokers without a binding court order. If this bill is passed, law enforcement will have to find other sources of "probable cause" for warrants. Given that the *Dobbs v. Jackson* decision was published less than a year ago and the average time for a trial to occur is 12-18 months after filing, it is unlikely that we will know the true number of women charged and convicted of accessing newly illegal reproductive care within the time frame of this project (McKinney Law Firm, 2022).

The CRS report would be the first step in revamping the anti-intrusion reform effort. Alone, the report cannot protect women in trigger law states. However, the report would make adopting the policy more likely as a key step in ensuring political feasibility. The CRS report and the subsequent political momentum could successfully shield women from warrantless access by law enforcement to personal data. Still, once some alternative probable cause is submitted to a court, women would have no protection from prosecutors using that data to build cases against them. As such, successfully passing a new version of S.1265 will remove approximately half of women's legal exposure. Still, law enforcement could find other forms of evidence that reveal a woman has recently accessed illegal reproductive care that could be equally damning in court.

The CRS report and political momentum that follows is somewhat effective at protecting the target population.

POLITICAL FEASIBILITY

On average, the CRS delivers over 400 policy-specific reports each year (Mazanec, 2021). Given that the CRS is responsible for responding to Congressional requests, as well as managing and delivering those reports, it is highly unlikely that a request from any of the previous S.1265 sponsors will be unmet. Bureaucratic incentives are aligned with the provision updates on major policy questions, suggesting the request is administratively robust. The bill, if passed, will indefinitely improve the digital protection of female users in trigger law states unless a court finds standing to overturn the law. It will likely outlast its enacting coalition given growing desires to prevent law enforcement from making unwanted advances into citizens' personal lives. According to a 2014 Pew Research Study "Privacy Perceptions," 80% of adults believe that Americans should be concerned about the government's monitoring of internet communications and that basic communication methods like texts and emails are not secure (Madden, 2014). Six years later, Pew found that six in ten American adults say they do not think it is possible to go through a single day without having data collected about them by the government (Auxier et al., 2019). This trend of concern is likely to continue until further legislative action is taken.

The sustained attention and support of lawmakers and additional momentum since Roe was overturned suggests an updated CRS report–and the anti-intrusion effort to follow– is highly feasible. The following section evaluates primary stakeholders' perspectives on this alternative.

Women of Childbearing Age

The AP found in the first half of 2020, federal, state, and local law enforcement agencies issued over 112,000 requests for data to Apple, Google, Facebook, and Microsoft–three times the number of requests submitted five years earlier (O'Brien & Liedtke, 2021). That year, reports surfaced that those agencies purchased geolocation data–without warrants or court orders–from analytics companies like Venntel, X-Mode, and Babel Street (Morrison, 2020). Those requests and purchases enabled deportations and arrests. Since Roe's reversal, a flood of Twitter activity has emerged, from the EFF's Director of Cybersecurity Eva Galperin's Tweeting "if you are in the U.S. and you're using a period tracking app, today is good day to delete it before you create a trove of data that will be used to prosecute you if you ever have an abortion," to over 6 million Tweets of warning from individuals expressing concerns over government access to online health information. Women of child bearing age fear the very same actions taken by law enforcement agencies in 2020 will be deployed today.

Business

S.1265 takes away the Attorney General's authority to grant civil immunity to providers and other third parties for assistance with surveillance not required or permitted by statute. Providers retain immunity for surveillance assistance ordered by a court. This bill would essentially shut down the clandestine business sector that trades individual information without court orders. Data brokers that profit off of the sale of this information and gain leverage over the government for providing that information will suffer losses. Otherwise, S.1265 will have a minimal impact on national, state, and local businesses, as most do not collect sensitive information that may be used in criminal court. Additionally, the price for each individual's data is low, worth merely $0.0005 per person (Jurcys, 2019). This indicates businesses that do sell sensitive data are losing little revenue without the ability to sell that information to law enforcement.

Advocacy Groups

In 2022, 50 consumer-rights and privacy-rights groups including the Brennan Center for Justice and the ACLU sent a letter to the Congress: “The Fourth Amendment’s warrant requirement protects not only our privacy, but our freedoms of association, religion and belief. The government should not be able to buy its way around fundamental rights. We call on the leaders of the Senate and House Judiciary Committees to hold hearings to expose the government’s activities and advance legislative solutions such as S.1265.” This majority-liberal coalition is joined by the conservative Alliance of Responsible Citizenship (ARC) spearheaded by Dr. Jordan Peterson. ARC expressed concern over “the extension of reach and control over even the most private details of our lives..; The use of increasingly powerful and invasive technology to monitor and control everything... can lead only to tyranny and despair. How do we forestall regulatory capture and the proclivity for government and corporation enterprises to collude at the highest levels and become authoritarian?” (Peterson, 2023). Advocacy groups– left, right, and libertarian alike– are calling for a bill like S.1265 to be proposed once again and passed.

Legislators

Since this bill was proposed in 2021 by Senators Wyden (D-OR), and Paul (R-KY), Sanders (D-VT) and 18 others, it has garnered widespread and bipartisan support. In 2022, the House Judiciary Committee hosted a hearing titled Digital Dragnets: Examining the Government’s Access to Your Personal Data. Rep. Nadler (D-NY) introduced the Honorable Bob Goodlatte, a former Republican Congressman from Virginia and Senior Policy Advisor at the nonpartisan Project for Privacy & Surveillance Accountability to discuss how “consumers may be somewhat ambivalent about the amount of information they are providing to companies, yet the government’s access to this information is far more ominous” (Goodlatte, 2022). Republicans in support of the bill include a wide range of actors, including Rep. Jordan (OH), Rep. Biggs (AZ), Rep. Gaetz. Democratic supporters include Rep. Lofgren (CA) and Rep. Scanlon (PA). However, there has been no movement since the Digital Dragnets hearing. The original coalition has neglected to connect digital autonomy to women's intimate data, so momentum could be generated once again if a new coalition were to connect the dots between information presented in the hearing and the lived experience of women fearful of their online exposure.

EQUITY

Equity is defined by equal distribution of benefits and challenges across people of every level of privilege and socioeconomic status, A CRS report of S.1265 would share information with the public and lawmakers to highlight its legislative obstacles and intended effects. An interview with Danielle Citron, a professor at the University of Virginia School of Law and expert in civil rights and feminist law, describes efforts to protect women from warrantless information grabs from third-party data brokers as the motivating force behind women's legal exposure: "There are three central actors that worry me and that implicate our intimate privacy. That's the corporate surveillance of intimate life. It's individuals surveilling and exploiting intimate privacy. And it's governments invading intimate privacy" (Oster, 2023). In her book The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (2022), Citron contends that federal law has struggled to keep up with the pace of privacy and reveals that "our current system leaves victims—particularly women, LGBTQ+ people, and marginalized groups—shamed and powerless while perpetrators profit, warping cultural norms around the world" (pg. 4) (Citron, 2022). Preventing warrantless government surveillance would create a new reality where "privacy is valued, and people are protected as they embrace what technology offers" (Wyatt & Citron, 2022). A federal law would extend these privacy protections to all regardless of state reproductive protections.

As a part of the broader anti-intrusion reform effort, S. 1265 would prevent law enforcement's access to and usage of all women's intimate data without a warrant, rendering this option fairly equitable.

COSTS AND BENEFITS

The cost of a report is low as such coverage is built into CRS operational costs. It will come with the opportunity cost of not completing a report on a different topic. However, the eventual signage of a newly proposed bill similar to S.1265 would impose some costs on data brokers who profit from the sale of this information. It is still unknown how many law enforcement requests have been made to data brokers since the *Dobbs v. Jackson* decision, and the price per provision of data is also unknown. In the Digital Dragnet House hearing, Elizabeth Goitein, Senior Director of the Liberty & National Security Program at the Brennan Center for Justice noted that the government currently can sidestep warrant requirements by merely writing "a big check" to access virtually unlimited quantities of data without suspicion of wrongdoing (Goodlatte, 2022). Ultimately, the number sales of individual's data, as well as the price of each of these, will be necessary to gauge the extent of government intrusion, the methods it deploys to do so, the costs to women, and the profits companies that sell this data make. It is still unlikely that the data sales brokers to law enforcement make up a large share of the total revenue. If law enforcement obtains probable cause without access to data, the financial impact on data brokers will be more limited. Given this effort's nonexistent cost to consumers, its financial impact is limited to a small subsection of data brokers, yet it would have a large impact on halting the first step by which law enforcement can target women seeking reproductive care. This option is inexpensive.

Alternative 2: Emergency FTC Funding

Each year, the FTC receives consumer complaints reporting abuses of privacy that it lacks the resources to manage. Last year, the FTC issued 22 new administrative complaints and entered 20 final administrative orders, but were unable to address thousands of violations of new offenders (Balser, 2022). To expand capabilities and address complaints stemming from emerging technologies and services tracking women's health, this alternative requires the FTC be empowered by additional funding. In one recent report, FTC identified a need for an additional $10,646,000 to manage digital privacy and health complaints (Ibid.).

Fiscal Year 2023's budget was signed into law in December, 2022. As such, the only way to provide supplemental funding is to attach a "rider"–an additional, often unrelated provision–onto the next emergency supplemental appropriations bill, whenever that opportunity appears. This requires TPCMMH to develop and contact a shortlist of Members who (1) have demonstrated interest in women's health issues; (2) have a record of attaching extraneous funding to appropriations; and (3) have indicated a willingness to dedicate political capital to privacy concerns. This requires leveraging TPCMMH's network to identify such a Representative through pre-existing political channels on and off the Hill and enlisting its research team to curate an informational portfolio to be deployed at the opportune moment to attach the rider.

EFFECTIVENESS

The FTC brought forth hundreds of enforcement actions to protect the security and privacy of consumers' personal information, some of which have included substantial civil penalties. The FTC's administrative complaints and final administrative orders were unable to address thousands of violations of new offenders (Balser, 2022). If a policy rider is attached to an upcoming emergency appropriations bill with the added $10,646,000 the FTC requested, the FTC will be able to address a number of–but not all–data privacy violations (Katsaros & Khan, 2022). With a $10.5 million dollar earmark, it can be assumed that at least one thousand new violations can be addressed.

There are a number of limitations to approximating the number of women that will seek and obtain financial redress for data privacy violations. First, given that Roe v. Wade was recently repealed, women in trigger law states are only beginning to report their concerns to the FTC, which has not released the number of reported issues. However, we can assume that the number is substantial, given that the FTC released a Mobile Health App Interactive Tool for consumers to navigate using apps like Flo and for companies to avoid breaking standards set by HIPAA, COPPA, or the FTC's Health Breach Notification Rule. Secondly, the downstream impact of the availability of resources for redress on women's comfort utilizing online services is unclear without data collected since the right to abortion was overturned. One NIH study completed in 2019 outlines women's preference for these services, characterizing them as "highly used and valued" given their trust in the anonymous network it provided and control it afforded them (Lupton, 2019).

Since Roe's reversal, Mozilla completed a study that found of ten pregnancy apps, ten period trackers, and five accessory devices, only seven had reputable privacy practices (Boyd, 2022). On the heels of the Forbes story which broke this news and the dozens which followed, it is safe to assume trust has been diminished.

The FTC's post-facto role in data privacy is only relevant *after* a violation has occurred. Women may feel more comfortable using all health apps knowing there is a system in place in the event of a violation, but given that a only third of Americans self-report paying "a great deal" of attention to politics, a policy rider may not make a large impact on the public consciousness (Fioroni & Reinhart, 2022). Companies, on the other hand, pay attention to trends in government spending and activity. Relevant enterprises may adjust their operations given intensified scrutiny, deterring unscrupulous activity and reducing the number of women in trigger law states whose sensitive health data is vulnerable. This option does not increase women's autonomy over who has access to that data, but it does improve control after a violation occurs.

This option is somewhat effective at defending women's data in trigger law states.

POLITICAL FEASIBILITY

Since earmarks were voted back into practice in 2021, over $15 billion dollars in earmarks have found their way into the federal budget (Wasson, 2022). Unfortunately, policy riders are unsustainable solutions that cannot provide support beyond their spending window. Once appropriated, the funds are not automatically incorporated into the upcoming fiscal year's budget. It's worth noting that this $10.5 million was briefly glossed over in the 2023 budget request. Neither the FTC nor the Biden administration submitted a formal request.

Despite this challenge, the FTC as a federal agency has some flexibility with implementation as well as substantial incentives to pursue claims to the submitter's satisfaction. Favorably aligned incentives pitted against fleeting resources creates a mixed bag for political feasibility. Given women of childbearing age and businesses' ambivalence or lack of knowledge about the rider coupled with advocacy group support and legislators' renewed ability to attach earmarks to bills, this alternative is somewhat politically feasible.

Women of Childbearing Age

Annual “budget justifications” tout the thousands of consumer complaints addressed and the millions obtained for them from violators. Last year alone, the FTC obtained over $470 million in refunds to consumers (Katsaros & Khan, 2022). These metrics are regularly released and help ensure the FTC moves quickly to address concerns. Given that many riders are tacked onto emergency appropriations for imminent crises, many fly under the public’s radar, distracted by whatever pressing national security situation, natural disaster, or public health catastrophe is unfolding. It is unlikely that most women of childbearing age in trigger law states will pay attention to fluctuations in FTC spending given national events, such as Russia invading Ukraine. Women who file following violations might be grateful if they are more likely to obtain monetary compensation given supplemented funding, but the general target population's response may range from pleased to ambivalent about the spending.

Business

Businesses may have little opinion about supplemental FTC funding. The FTC has ramped up crackdowns on UDAAPs violations. According to the FTC’s “Legal Library: Cases and Proceedings” website section, “every year the FTC brings hundreds of cases against individuals and companies for violating consumer protection and competition laws that the agency enforces.” However, it is unknown how many investigations are conducted per year. Regardless, the vast majority of American businesses will not be troubled by FTC funding for activities that do not concern their enterprise.

Advocacy Groups

Over the last 14 years, FTC staffing has hardly increased while the number of employees in major tech companies has exponentially increased. For example, in 2021 the FTC had only 1,100 full-time employees–a substantially decrease from 1,746 in 1979–compared to Facebook's 60,000 (Facebook Reports Fourth Quarter and Full Year 2020 Results, 2021). In September of that year, 26 civil rights, civil liberties, and consumer protection organizations encouraged the House Committee on Energy and Commerce to allocate at least $1 billion to bolster FTC efforts to protect data privacy and prevent security abuses: "For far too long, Congress has failed to sufficiently fund the FTC to do the massive job with which it is tasked. The agency is overdue for an influx of resources to help it play catch-up to the modern economy" (Access Now et. al, 2021). These organizations included the ACLU, Consumer Reports, the Open Technology Institute, the Center for Digital Democracy, and many more. Although women's advocacy groups are yet to recommend this particular alternative, active D.C. advocacy groups more broadly have continued to express support.

Legislators

In December of 2022, Congress cleared a $1.7 trillion funding bill with $47 billion in funding to the Ukraine, as well as funding for over 7,000 targeted spending measures ranging from changing how electoral college votes are tabulated to deregulating the lobster industry (Wasson, 2022). Although the exact timing of a new rider may be unpredictable given the unexpected nature national emergencies, the likely usage of riders as leverage for politicians eager to add their own 'pet projects' is favorable. Champions who may be keen to attach the rider include either Representatives Frank Pallone (D-NJ) or Cathy McMorris Rogers (R-WA), both of whom have attempted to push data privacy bills through Congress. Both have been effective coalition-builders, but have been unsuccessful at passing more substantive measures. This could represent a minimally viable last resort to achieve their legislative goals.

Either lawmaker could be receptive to finding a way to bolster consumer protections, regardless of the legislative vehicle. Other lawmakers may similarly be keen to express their support for this rider in exchange for their own. The current congressional ecosystem is an advantageous environment for such a rider to enter and survive the legislative process.

EQUITY

Even with additional resources, the system designed to enable the filing of UDAAPs violation will not reach every woman. Many will not be aware that filing a UDAAPs complaint is possible or that such a system exists. Even if they were aware, the FTC still won't be able to address every requested investigation given resource constraints. A basic online search leads to a series of FTC and Consumer Finance Protection Bureau (CFPB) videos designed to guide consumers who suspect they have suffered a violation. Both videos describe why, how, and where to file a UDAAPs violation. Neither of the videos referenced information about health app-related UDAAPs violations.

However, if users continue through the process, they are offered the opportunity to describe the issue, offer what they think a fair resolution to the problem might be, and include a timeline of what they have done to independently resolve the issue. There may be confusion as the FTC is responsible for managing UDAAPs violations, yet the actual filing process occurs through the CFPB. Both the files and the videos were relatively intuitive. I, as well as 10 colleagues, filled out UDAAPs violation requests. The average time required to locate, decipher, and complete the form was 20 minutes and 45 seconds without prior provision of the link. However, all of these colleagues (1) spoke English as a primary language, (2) were somewhat familiar with and trusted government institutions to manage the process, and (3) were provided the words "unfair, deceptive, and abusive practices" and "complaint" to aid their search. This suggests that for those working hourly jobs (where the cost of time spent searching the web is more expensive than those working salaried jobs), those unaccustomed to navigating a government website, or those who do not know the formal terms that describe their situation, this time may be much longer.

Given this alternative's mixed accessibility, it is moderately equitable.

COSTS AND BENEFITS

This option is relatively cheap, but its effectiveness is also limited to the women resources will reach. According to the CFPB, last year 192 million people were eligible for relief after reported UDAAPS violations, leading to a total of 20 enforcement actions and the provision of $16 billion in consumer relief and $3.7 billion in civil penalties. So far, there have been 3 million UDAAPs violations reported to the Consumer Financial Protection Bureau this year (Enforcement by the Numbers, 2023). Some unknown fraction of that number represents UDAAPs violations related to health-related data apps. As such, the additional $10 million requested by the FTC may potentially pale in comparison to the actual scale of unreported violations. Without information about how many reported violations have been tied to information sold to data brokers, we cannot estimate the cost-effectiveness of this option. As more data is collected documenting the scale of the issue, future funding may be easier obtained than it currently is.

Regardless, we can assume that if the rider is sufficiently specific in targeting women dealing with reproductive health violations, this option presents a reasonably inexpensive way to manage the FTC's most egregious violations.

Alternative 3: Data Privacy Bill of Rights

TPCMMH may consider revamping the movement to defend data privacy via new legislation. It must first identify key lawmakers supportive of more stringent consumer protections on apps and online services, but who are also reticent to support the ADPPA, fearful its wide scope will prevent its passage. TPCMMH would foster relations with Congressional actors like House Energy and Commerce Committee Leader Cathy McMorris Rodgers (WA-05), Leader of the Consumer Protection and Commerce Subcommittee, Gus Bilirakis (FL-12), as well as the "My Body, My Data Act" (H.R.8111) sponsor, Representative Sara Jacobs (CA-51). Timing depends on the failure of the ADPPA, but the primary concern is coalition-building following an analysis of the previous bill's language and failure to meet bipartisan expectations for economic benefits and women's welfare. This bill would include a 2-year phase-in period for the following provisions:

1. **The right to be informed**: This requires businesses provide individuals with clear and concise information about when data is collected, the category and specifics of that information, the purpose for its processing, and contact details for company representatives. Provision must be completed in a timely manner and full profiles must be delivered so long as they are retained. See Table E in the Appendix.
2. **The right to opt-out**: This enables users to exclude themselves from data collection from that point forward. See Table F in the Appendix.
3. **The right to delete**: This empowers users to request companies delete their personal information and instruct service providers to do the same. This entails specification of data collected within a time frame or with respect to a certain activity. See Table G in. the Appendix.
4. **The right to rectify**: This allows users to supplement incomplete data or to correct inaccurate information. See Table H in the Appendix.
5. **The right to private action**: This allows consumers to sue a business for noncompliance with data protection laws. Unlike previous bills, this option would include monetary compensation for victims. This final provision is not included in the "simplified" DPBR in the outcomes matrix given its opposition from the business community. See Tables I and J in the Appendix.

EFFECTIVENESS

The Data Privacy Bill of Rights (DPBR) would protect the data privacy of millions of Americans. For the 20.9 million women in trigger law states, the bill enables them to take control of the information collected and sold to law enforcement that could lead to criminal charges if they access newly illegal reproductive care. Women will be able to deny companies the ability to collect and sell their data completely. In the event that women have adjusted their privacy settings to prevent collection and sale of their sensitive data, there will be no information for law enforcement to scrub off those platforms. The amount of sensitive data available for resale will be substantially reduced, and women's legal exposure to law enforcement will shrink insofar as women actually change their privacy settings.

This is likely, as one study finds women are more likely than men to say they would like access to additional layers of online protection. Women (62%) were more likely than men (49%) to personalize their privacy settings, and after experiencing a security problem, women (61%) were more likely than men (51%) to initiate permanent changes in their online behavior to protect themselves from future vulnerabilities (Murnane, 2016). This suggests that when provided with the option for additional layers of protection, women will likely take advantage of the opportunity.

Since the aforementioned study was completed approximately 7 years ago, women–especially those where reproductive care is restricted–are better informed and therefore more likely to make use of personalized privacy settings given growing concerns about data privacy. One study finds that 13% of apps collect data before obtaining consent and 87% of apps share user data with third parties with no method of discovering what information was obtained (Alfawzan et al., 2021). We estimate that women in trigger law states rates of privacy setting adjustment will jump from 62% in 2016 to at least 75% today as a conservative estimate (Pew Research Center, 2019). This means that of the 20.9 million women of childbearing age in trigger law states, 15.7 million will decide to take steps to protect themselves. We can safely assume that if this law is passed, many more women will be shielded from law enforcement's access to that information, especially since news coverage of online health information used as evidence in criminal cases can be categorized as impetus for "making lasting changes" in order to protect oneself from "future problems" (Murnane, 2016).

The private right to action (PRA) will help ensure that in the event that the aforementioned protections are violated, women will have a legal avenue to defend themselves from allegations in court and pursue redress for the costs and damages incurred as a result. With a PRA, lawsuits could be brought for violations "of sections 102 (loyalty duties), 104 (loyalty to individuals with respect to pricing), 202 (transparency), 203 (individual data ownership and control), 204 (right to consent and object), 206(b)(3)(C) (rights around third-party collecting entities), 207(a) (civil rights protections), 208(a) (establishment of data security practices), and 302 (service providers and third parties)" (Donovan-Smith, 2022). The PRA will close any remaining gaps in protection the DPBR otherwise cannot prevent.

The DPBR–with and without the PRA– would be highly effective.

POLITICAL FEASIBILITY

Passing the DPBR would be the most sustainable policy option as it would require a formal challenge in the court system to overturn. It would long outlast its enacting coalition and its benefits would be nearly immediate depending on phase-in periods for various provisions.

Sustained bipartisan support for a national data privacy standard coupled with recent momentum render the DPBR moderately politically feasible with the PRA and highly feasible without it.

Women of Childbearing Age

Since Roe's reversal, human rights bodies representing women from the U.N. to Planned Parenthood have sounded the alarm to push lawmakers into passing a data privacy bill. The U.N. stated "[Our] role is to outline clear guidelines on how to protect against gender based privacy infringements, to try and help prevent the ongoing harms experienced by many individuals and communities around the world...as people have lost confidence in their ability to safely participate." (Cronin, 2022) One consulting company conducted a survey of 2,028 internet users and found that women felt markedly less confident (52%) than men (33%) that they were protected from security problems (Murnane, 2016). It's likely that since these results were published, the current figures are much higher. Women of childbearing age in trigger law states are likely to absorb information from elite institutions such as the U.N. and generate sizable support for the DPBR hoping to be better protected from security threats.

Business

Given that many businesses would benefit from deregulatory legislation, bills with rights to access, opt-in, rectification, and deletion, have faced opposition from organizations like the Business Roundtable, which wrote to the ADPPA's sponsor, Rep. Pallone saying "several of its provisions would place unnecessary and economically harmful burdens on businesses without providing commensurate benefits to consumers" (Silverberg, 2022). Business advocates such as The Chamber of Commerce adamantly oppose any bill "that creates a blanket private right of action." The Chamber wrote to the members of the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce outlining concerns with a PRA "that would encourage abusive class action lawsuits through private rights of action...[where] there is an incentive for plaintiffs' attorneys to generate cases" ("U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action," 2022). These present serious financial obstacles for many industries.

Advocacy Groups

Technology advocacy groups such as the Information Technology and Innovation Foundation support a "targeted" approach, recommending their own skeleton framework excluding the PRA (McQuinn & Castro, 2019). However, Alan Butler, president of the Electronic Privacy Information Center Tweeted they would be "disappointed" by compromises to PRA access. Still, tech lobbyists have not launched a comprehensive campaign to kill a federal bill. Adam Kovacevich, the CEO of Chamber of Progress, points out that even the bill's liberal critics acknowledge it goes beyond any of the state laws it would preempt — even California's: "I don't think anyone in industry is crazy about the idea of the private right of action, the idea of more lawsuits," he says. But, he adds, "tech companies have already spent years learning to comply with the growing web of privacy regimes around the world– A somewhat stricter law might not be so bad if it provides a clear, fixed national standard" (Edelman, 2022).

Legislators

Broadly, legislators support data privacy reform. The House Commerce Committee advanced the ADPPA by a 53-2 margin in December of 2022. This bipartisan consensus bodes well for the DPBR considering the newly switched Ranking Member and Chairman dyad Rep. Rogers and Pallone tag-teamed the ADPPA as the decade's most successful data privacy bill. However, Senator Cantwell (D-WA) – whose support is necessary as Chair of the Senate Commerce, Science and Transportation Committee– stated "she couldn't support the bipartisan framework unless House lawmakers limit forced arbitration and create a right for individuals to sue violating companies" (Donovan-Smith, 2022).

A phase-in period of 1 year–3 years quicker than the ADPPA–could appease Cantwell. However, omitting the PRA is pivotal to the support of business, most of which foresee federal privacy regulation on the horizon. Omitting the PRA addresses their concerns over frivolous lawsuits. Given Cantwell's power, it would be prudent to include her statutory damages of "$100 to $1000 per violation per day, or actual damages, whichever is greater" (Lima, 2022). This increase the bill's potential for successfully exiting the committee without frustrating industry lobbies and decreasing floor votes.

EQUITY

A simplified federal data privacy standard will distribute benefits equally across women in trigger law states, because the ability to access those benefits are largely managed on the back-end of the service or site provider. Specifically, companies will have to complete the technological legwork to verify and complete consumer requests, whereas any tech savvy woman between the ages of 15-44, all of whom grew up in the era of the internet, will be able to locate and access data protection settings on websites. The required actions are limited to a few clicks, rendering the 'hassle factor' minimal. However, the PRA presents some equity issues. Specifically, pursuing claims in the court of law requires significant resources, time (an opportunity cost), and patience. The California Business Journal suggests that the average simple suit costs $10,000 in legal fees alone (Lawsuit Basics: How Much Does It Cost To Sue Someone?, 2020). Although the PRA is designed to make seeking compensation for damages more accessible for women, this price tag is a serious barrier to take-up.

The DPBR is highly equitable without the PRA and equitable with the PRA.

COSTS AND BENEFITS

The DPBR is not being considered in response to *Dobbs v. Jackson* per se. Rather, it is a measure designed to decrease the costs of adhering to a complex patchwork of data privacy laws across states. As such, the primary costs accrue to businesses and the beneficiaries are the average internet consumer rather than women of childbearing age in the 13 trigger law states. Considering costs in a more holistic manner, weighing total costs and benefits accrued by businesses against the costs and benefits to women in trigger law states better captures the protection of our target population.

Compliance costs include about $6 billion in compliance personnel, $40 million in privacy audits, $5 billion in data infrastructure, $274 million in data access, $340 million in data opt-out capabilities, $780 million in data deletion verification and processing, and $55 million in data rectification. The market inefficiencies of less access to data and lower ad effectiveness will cost a combined $79 billion. According to the ITIF, the cost of including the PRA will cost an additional $2.7 billion. Total costs of a simplified DPBR are estimated at $93 billion, and with PRA would cost $95 billion.

Fifty-five–a data consulting company– estimates that passing the federated law could have a trillion-dollar positive impact over the next decade (Tollet, 2021). Still, within this election cycle, the short and medium-term financial impact compared to the impact on 20.9 million women in question is expensive. These are the highest-priced alternatives and represent between $93-95 billion in costs to the American economy in the first year. [See Appendix A]

Without the PRA, this alternative is expensive, and with the PRA, it is the most expensive option.

Recommendation

Given TPCMMH's priorities of effectiveness, political feasibility, equity, and costing, the combination of the updated S.1265 CRS Report and the DPBR without the PRA is recommended. Although the PRA would afford women more autonomy to obtain monetary damages following violations of privacy, the expense renders the price to pursue retribution too great to be equitable and would generate sufficient opposition from the business community to kill the bill and, in the process, deny women the opportunity to enjoy any rights to privacy. Moving forward, re-examining The Fourth Amendment Is Not For Sale Act through a CRS report would revitalize the broader anti-intrusion movement to prevent women's data from entering law enforcement's hands to begin with, while the simplified DPBR would empower them to manage their own data usage and prevent its collection altogether. These options represent the most holistic approach to safeguarding against the weaponization of women's data.

OUTCOMES MATRIX

Alternatives	Effectiveness	Political Feasibility	Equity	Costs v. Benefits	Total Points
CRS Report	**Somewhat Effective**	**Highly Feasible**	**Equitable**	**Inexpensive**	**12**
Emergency FTC Funds	Somewhat Effective	Somewhat Feasible	Moderately Equitable	Inexpensive	8
Data Privacy Bill of Rights *Simplified Model*	**Highly Effective**	**Highly Feasible**	**Highly Equitable**	**Expensive**	**13**
Data Privacy Bill of Rights *w/PRA*	Highly Effective	Moderately Feasible	Equitable	Very Expensive	8

Color Coding & Point System (5-Point Scale)

Color	Dark Purple	Purple	Lavender	Soft Pink	Hot Pink
Point Value	0	1	2	3	4

Implementation

TPCMMH's role as an advocate is to provide information, create policy analysis, generate media attention, and galvanize public support for the recommended alternatives. Implementation guidance follows two parallel approaches. The first, commissioning and generating public support for a re-examined CRS report on S.1265, and second, managing the proposal, shepherding the legislation, and monitoring implementation.

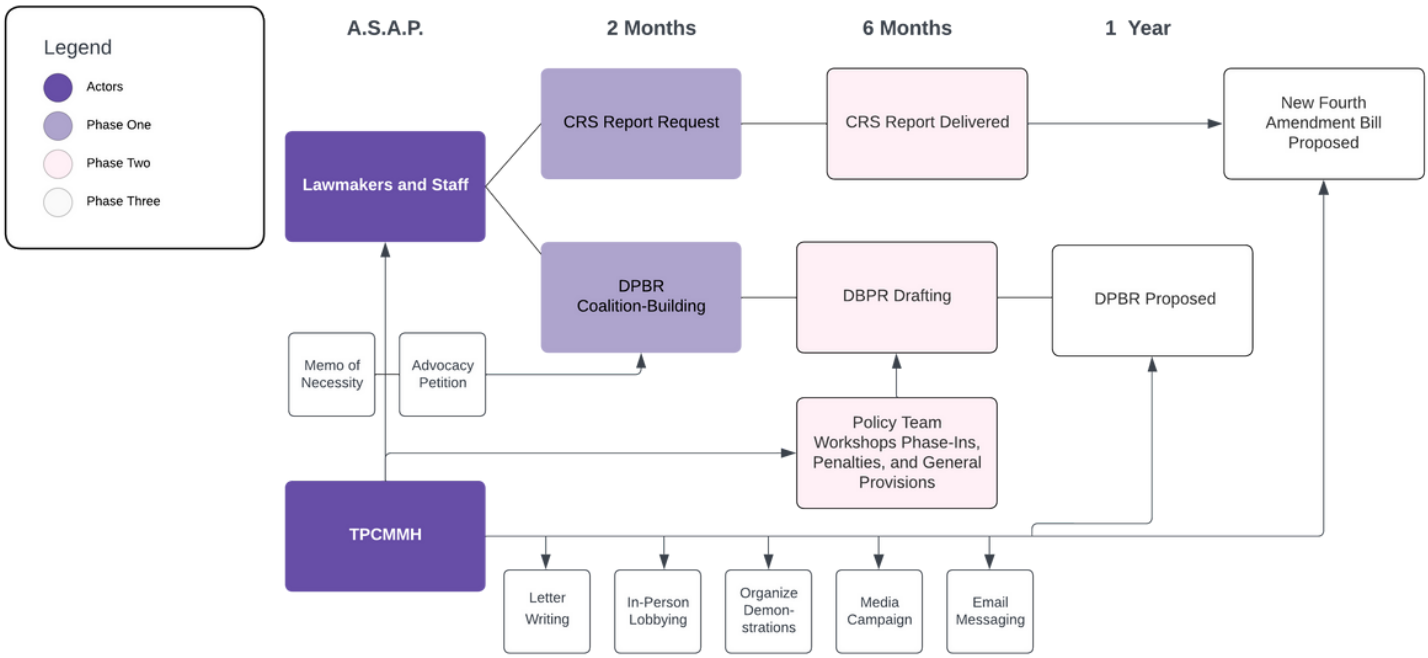


Figure 3: Shepherding the CRS Report and DPBR Timeline

1. CRS Report and Advocacy Efforts

As soon as possible, the TPCMMH team must convene to discuss the contents of the DPBR and construct a "messaging bible" to bring team members up-to-speed and make sure they consistent when talking to political actors. This is especially important with regard to why the PRA is an effective but infeasible addition to the DPBR. Then, they will publicize and collect "e-signatures" for a petition through its email list requesting a Representative to commission a women-centric Fourth Amendment report, which will be linked on TPCMMH's social media platforms (Facebook, Instagram, Twitter, and LinkedIn).

Then, TPCMMH must connect with the most likely actor to request the report. For our purposes, Rep. Sara Jacobs, who proposed the My Body My Data Act, represents TPCMMH's best option given her prioritization of women's data post-Roe. If Jacobs declines the proposition, the team will reach out to Senator Cantwell and Rep. Frank Pallone, both of whom previously indicated support for data privacy. TPCMMH will produce a memo to inform the congressional study, including an ideal submission date, which would be best timed with the *Dodds* decision's anniversary in July.

It is incumbent upon TPCMMH to continue to elevate the conversation surrounding the weaponization of data against women in the public consciousness. The majority of TPCMMH's role throughout the report development process and after publication is to broaden coalition support by co-writing letters with other women's advocacy organizations, including the Center for Reproductive Rights, the National Women's Law Center, the Association for Women's Rights in Development, the League of Women Voters, and Equality Now, all of which have recently released statements about women's data privacy. These names represent the first wave of like-minded coalition-leaders to create momentum for media attention and apply legislative pressure. In conjunction with these entities, TPCMMH will regularly meet with lawmakers. The content of such meetings will be fodder for a media campaign, including videos (with lawmaker permission), Tweeted quotes of support, and site blogs highlighting relevant topics and trends.

One wrench in this plan is the possibility of an exogenous shock such as a national security crisis that may have been prevented by law enforcement's unfettered access to third-party data broker information. It is possible that a bad actor presents signs of concerning behavior online yet on no other media, and law enforcement would be denied probable cause for an arrest warrant. This may enable a terrorist attack or insurgency efforts. People may die, property may be destroyed, institutional credibility may be damaged, and our international reputation may be jeopardized. It could be necessary to include a safety valve provision which stipulates that threats to national security–as opposed to violations of state law– allow law enforcement to bypass warrant requirements for data access. However, TPCMMH must avoid subversion of its original legislative intent through regulation specificity.

2. DPBR Advocacy and Support

It is recommended that TPCMMH develop a memo to be sent to Congress describing the urgent necessity of the DPBR's proposal and passage, the impact the law would have on women in trigger law states, and the potentially disastrous consequences of failing to do so. This will be accompanied by the petition of individual and organization's e-signatures echoing similar concerns.

Throughout the coalition-building, drafting, and proposal process, TPCMMH will continue to write and publish related letters through their email listserv and on social media, schedule meetings with lawmakers, and continue an aggressive media campaign by filming videos with women facing criminal charges in trigger law states. One of the most logistically complicated matters will be co-organizing demonstrations in front of Capitol Hill similar to the 2017 Women's March on Washington (National Museum of American History, 2020). The Women's March organization– which formed to plan the March– has since conducted 26 state and federal-level marches with themes like the Digital Defenders March in 2019 and the Bigger Than Roe Women's March of 2023. Given their massive 600k following on Twitter, a partnership will help publicize efforts to move the DPBR forward.

However, this bill could face opposition from the business community. Given the relative cost of adjusting to new data practices and adapting online infrastructure, it will be important to offer affected businesses ample guidance and accessible information to avoid accidental noncompliance. For this, we look to the implementation of the California Consumer Privacy Act. California.gov released multiple blogs describing the obligations of affected companies and the timeline with which they must adhere to requirements (Friel & McLellan, 2019). TPCMMH's policy team--namely, Sarah Johanek, Policy Project Manager, Rebecca Britt, Director of Research and Impact, and Mary Miller, Advisor of Strategic Partnerships--should workshop Q&A adapting CCPA guidance to the new DPBR, as well as workshop questions for women in trigger law states who are eager to understand their new rights. Business-related questions include:

- Does the DPBR apply to my business?
- What do I do if my state has stricter privacy provisions than the DPBR?
- What are the potential penalties for violations?

Questions for women in trigger law states may include:

- What new rights will the DPBR grant me?
- What happens if I can't locate an app's privacy policy?
- How can I access/verify the information a company has collected about me?
- Can I go back and delete information that was collected before the DPBR was enacted?
- What tools and information are companies expected to provide?

An answer for the final question could be: Businesses must provide a categorical description of personal information collected in the past year; the commercial purposes explaining why the personal details are collected; the names of the third parties with whom personal information is shared; a link to a "Do Not Sell My Personal Information" opt-out tool; and at least two methods for submitting data access requests (Friel & McLellan, 2019).

Contributing to a comprehensive guide for businesses as well as the target population will help ensure information flows freely to the affected stakeholders, ameliorating concerns and jumpstarting compliance ahead of phase-in periods.

However, verifying compliance may prove difficult. Lawmakers should consider adding stipulations with funding for regular compliance audits conducted by consultants like Deloitte or BCG who regularly support the public sector in ensuring regulation adherence. TPCMMH also should consider encouraging independent organizations such as Consumer Reports or the EFF to conduct thorough examinations of company policy and consumer access to DPBR rights. Both consultants and independent organizations could serve as lawmakers and TPCMMH's "eyes and ears" to identify noncompliance. The redundancy of multiple actors monitoring post-passage outcomes can help identify necessary amendments or tweaks.

Conclusion

Following the Dobbs v. Jackson decision overturning the right to abortion, law enforcement is scrubbing intimate health data to discern if women in "trigger law" states accessed newly unlawful reproductive care. If we fail to protect women's sensitive data, 1 in 3 American women of child-bearing age face legal exposure from information sold by data brokers to law enforcement ("U.S. Census Populations with Bridged Race Categories," 2022). Businesses and consumers alike must understand how, why, and by whom personal information collected, processed, used; be empowered to take control of their privacy settings; and rest assured that law enforcement will not have unfettered access to their intimate online information. This report considers the following options to reduce information exposure and increase women's digital autonomy:

- A renewed look at the Fourth Amendment is Not For Sale Act (S.1265), which would outlaw searches and seizure of online information without a warrant;
- Allocate emergency FTC funding for unfair, deceptive, or abusive uses of women's online data;
- Proposing a Data Privacy Bill of Rights to allow people to access, alter, or delete data as well as opt-out of data collection;
- And propose the DPBR with the private right to action, allowing victims of data abuses to pursue monetary redress for failures to comply with the DPBR.

This report recommends a combination of the first and third options. While additional refinements and clarifications of the DPBR and revamped versions of S.1265 are likely to occur throughout the drafting process, it is important that fundamental components reflect this new era of consumer privacy rights which has dawned in America.

This report recommends that TPCMMH begin engaging with the lawmakers most critical to proposing and passing the necessary legislation, collecting online petition signatures, developing a media kit, and generating support on the Hill through calls and scheduled in-person meetings.

References

815 ILCS 530/ Personal Information Protection Act. (2013). Retrieved from Illinois General Assembly website: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

Access Now, ACLU, Asian Americans Advancing Justice, Center for American Progress, Center for Digital Democracy, Center for Democracy and Technology, ... Lawyer's Committee for Civil Rights. (2021, September 23). Group letter in support of FTC privacy funding.

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2021). Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: A Scoping Review and Content Analysis (Preprint). JMIR MHealth and UHealth, 10(5). https://doi.org/10.2196/33735

Ali, S. S. (2022, June 24). Prosecutors in states where abortion is now illegal could begin building criminal cases against providers. Retrieved July 6, 2022, from NBC News website: https://www.yahoo.com/video/prosecutors-states-where-abortion-now-231745604.html guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABIm0mG8e1DS0ZXe1_oWjt2BG5RytcpvGiieiiXkabQYXqpsptwN-PJoo8ItZyWl5dSGYr75E5aK6IaI5oBMD-nD15LGCT1LxKXY50gV2gfiTFBA10Z_v5L4aR_B70J9mWS_-0mjm7aP35Ffm5SpEpim9wdHbg3HjKj2ChyB6B5V

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved March 9, 2023, from Pew Research Center website: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Balser, J. (2022). Overview of Governmental Action Under the Stored Communications Act (SCA). In *Congressional Research Service* (pp. 1–3). Washington, D.C.: Congressional Research Service. Retrieved from Congressional Research Service website: https://chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://crsreports.congress.gov/product/pdf/LSB/LSB10801

Baumann, J. (2022, May 18). Fertility Apps Bound by Weak Disclosure Rules in Post-Roe World. Retrieved April 7, 2023, from Bloomberg News Law website: https://news.bloomberglaw.com/pharma-and-life-sciences/fertility-apps-bound-by-weak-disclosure-rules-in-post-roe-world

Bertini, M., & Wathieu, L. (2010, May). How to Stop Customers from Fixating on Price. Retrieved from Harvard Business Review website: https://hbr.org/2010/05/how-to-stop-customers-from-fixating-on-price

Bogdan Botezatu. (2018). More Organizations Are Adopting Biometrics for Security—But Barriers Still Remain. Retrieved from Bitdefender.com website: https://businessinsights.bitdefender.com/more-organizations-are-adopting-biometrics-for-security-but-barriers-still-remain

Boyd, A. (2022, August). Make smart choices to protect your privacy. Search for products. Read expert reviews. Get tips and tricks. Retrieved March 1, 2023, from Mozilla Foundation website: https://foundation.mozilla.org/en/privacynotincluded/categories/reproductive-health/

Brown, M. (2019). Legal Reform News and Events. Retrieved February 26, 2023, from U.S. Chamber of Commerce Institute for Legal Reform website: https://www.instituteforlegalreform.com/uploads/sites/1/Class_Action_Study.pdf

Burkhard, J. (2023). About 2020 Mom. Retrieved April 1, 2023, from The Policy Center for Maternal Mental Health website: https://www.2020mom.org/our-work

California Consumer Privacy Act (CCPA). (2018, October 15). Retrieved from State of California - Department of Justice - Office of the Attorney General website: https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act

References

Carraro, M. (2018, November 12). GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey. Retrieved April 7, 2023, from www.businesswire.com website: https://www.businesswire.com/news/home/20181112005447/en/GDPR-Burdens-Hinder-MA-Transactions-in-the-EMEA-Region-According-to-Merrill-Corporation-Survey

Cases and Proceedings. (2023, March). Retrieved March 1, 2023, from Federal Trade Commission website: https://www.ftc.gov/legal-library/browse/cases-proceedings

Castro, D., Dascoli, L., & Diebold, G. (2022, January 24). The Looming Cost of a Patchwork of State Privacy Laws. Retrieved from Information Technology & Innovation Foundation website: https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/

Chen, B. X. (2021, March 31). If You Care About Privacy, It's Time to Try a New Web Browser. *The New York Times*. Retrieved from https://www.nytimes.com/2021/03/31/technology/personaltech/online-privacy-private-browsers.html

Chin, V., Marcil, S., Daniel, C., & Hemmige, H. (2023). Public Sector Services. Retrieved March 2, 2023, from BCG Global website: https://www.bcg.com/industries/public-sector/overview

Chivot, E., & Castro, D. (2019, June 17). What the Evidence Shows About the Impact of the GDPR After One Year. Retrieved from Center for Data Innovation website: https://datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/

Christie, A. (2020, August 17). Australia - Data Protection Overview. Retrieved from DataGuidance website: https://www.dataguidance.com/notes/australia-data-protection-overview

Clement, J. (2018). Topic: Internet usage in the United States. Retrieved March 1, 2023, from Statista website: https://www.statista.com/topics/2237/internet-usage-in-the-united-states/

Coalition Calls for Congressional Hearings on the Fourth Amendment Is Not For Sale Act. (2021, April 20). Retrieved January 7, 2023, from American Civil Liberties Union website: https://www.aclu.org/letter/coalition-calls-congressional-hearings-fourth-amendment-not-sale-act

Cohen, K. (2022, July 11). Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data. Retrieved from Federal Trade Commission website: https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal

Consumer-Advocacy, Media-Justice and Privacy-Rights Groups Call on Congress to Kickstart the Fourth Amendment Is Not for Sale Act [Letter to Dick Durbin, Chuck Grassley, Jerry Nadler, & Jim Jordan; Email]. (2022, June 26).

Cosgrove, C., Lively, T., Adams, S., Wang, I., & Fazlioglu, M. (2023). Privacy Rights By State. Retrieved March 2, 2023, from Westin Research Center website: https://iapp.org/news/westin-research-center/#

Country Business Patterns: 2020 SUSB Annual Data Tables by Establishment Industry. (2020). Retrieved March 1, 2023, from Census.gov website: https://www.census.gov/data/tables/2016/econ/susb/2016-susb-annual.html

Coutts, S. (2018, October 14). Anti-choice groups use smartphone surveillance to target 'abortion-minded women' during clinic visits. Rewire News Group.

Cronin, S. (2022, July 23). Gender equality in the right to privacy – an essential for all. Retrieved March 1, 2023, from United Nations Human Rights Office of the Commissioner website: https://www.ohchr.org/en/press-releases/2020/03/gender-equality-right-privacy-essential-all

References

Danielle Keats Citron. (2022). The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age. W. W. Norton & Company. Retrieved from https://wwnorton.com/books/9780393882315

Dashlane. (2015, July 21). Online Overload – It's Worse Than You Thought. Retrieved March 1, 2023, from Dashlane website: https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought

Data Analyst Salaries. (2023, July 3). Retrieved February 27, 2023, from Glassdoor website: https://www.glassdoor.com/Salaries/data-analyst-salary-SRCH_KO0,12.html

Data Sharing and Open Data for Banks A report for HM Treasury and Cabinet Office Data Sharing and Open Data for Banks --A report for HM Treasury and Cabinet Office. (2014). In Open Data Institute and Fingleton Associates. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF

David Leo Weimer, & Vining, A. R. (2017). Policy analysis : concepts and practice (6th ed., pp. 280–303). New York: Routledge, Taylor & Francis Group.

Deighton, J., & Johnson, P. (2015, December). The Value of Data. Retrieved February 21, 2023, from Direct Marketing Association and the Data-Driven marketing Institute website: https://thedmaorg/wp-content/uploads/Value-of-Data-Summary.pdf

Diamant, J., & Aleksandra Sandstrom. (2020, January 21). Do state laws on abortion reflect public opinion? Retrieved January 23, 2020, from Pew Research Center website: https://www.pewresearch.org/fact-tank/2020/01/21/do-state-laws-on-abortion-reflect-public-opinion/

Donovan-Smith, O. (2022, July 5). McMorris Rodgers, House Democrats back compromise to pass historic privacy bill. But will Cantwell let it pass? | The Spokesman-Review. Retrieved from The Spokesman-Review website: https://www.spokesman.com/stories/2022/jul/25/historic-data-privacy-law-could-be-within-reach-if/

Edelman, G. (2022, July 21). Congress Might Pass an Actually Good Privacy Bill. Retrieved February 28, 2023, from Wired website: https://www.wired.com/story/american-data-privacy-protection-act-adppa/

Editorial Staff. (2020, July 15). Lawsuit Basics: How Much Does It Cost to Sue Someone? - California Business Journal. Retrieved March 1, 2023, from The California Business Journal website: https://calbizjournal.com/lawsuit-basics-how-much-does-it-cost-to-sue-someone/#:~:text=It

Enforcement by the Numbers. (2023, February). Retrieved February 23, 2023, from Consumer Financial Protection Bureau website: https://www.consumerfinance.gov/enforcement/enforcement-by-the-numbers/

European Union - Data Privacy and Protection. (n.d.). Retrieved October 7, 2022, from Trade.gov website: https://www.trade.gov/european-union-data-privacy-and protection#:~:text=The%20EU%20General%20Data%20Protection

Facebook Reports Fourth Quarter and Full Year 2020 Results. (2021, January 27). Retrieved March 1, 2023, from Facebook website: https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year2020-Results/default.aspx.

Fioroni, S., & Reinhart, R. (2022, February 17). Americans' Attention to National News Lowest in Four Years. Retrieved March 1, 2023, from Knight Foundation website: https://knightfoundation.org/articles/americans-attention-to-national-news-lowest-in-four-years/

Flo Health, Inc. (2020, October 15). Retrieved from Federal Trade Commission website: https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc

Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA). (2019). Retrieved March 2, 2023, from cppa.ca.gov website: https://cppa.ca.gov/faq.html

References

Friel, A., & McLellan, M. (2019). The California Consumer Privacy Act: Frequently Asked Questions. Retrieved March 12, 2023, from CCPA FAQ website: https://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bakerlaw.com/webfiles/Privacy/2019/Briefs/California-Consumer-Privacy-Act-FAQs.pdf\

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

Gallagher, B. (2020, December 21). The Need for Federal Data Privacy Laws in the U.S. | GDPR | I.S.P. Retrieved from IS Partners LLC website: https://www.ispartnersllc.com/blog/us-nationwide-data-privacy-law-gdpr/

Gebhart, G., & Barnett, D. (2022, June 30). Should You Really Delete Your Period Tracking App? Retrieved from Electronic Frontier Foundation website: https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app

Goldfarb, A., & Tucker, C. E. (2011). Privacy Regulation and Online Advertising. Management Science, 57(1), 57–71. https://doi.org/10.1287/mnsc.1100.1246

Good, T. (2019, January 23). What is the Cost of a HIPAA Audit?

Goodlatte, B. (2022). Digital Dragnets: Examining the Government's Access to Your Personal Data. In Congress.gov. House Judiciary Committee. Retrieved from House Judiciary Committee website: https://www.congress.gov/event/117th-congress/house-event/115009

Google Transparency Report. (2019). Retrieved March 1, 2023, from transparencyreport.google.com website: https://transparencyreport.google.com/eu-privacy/overview?hl=en

Government & Public Services. (2023). Retrieved March 2, 2023, from Deloitte website: https://www2.deloitte.com/us/en/pages/careers/articles/join-deloitte-government-and-public-services.html?id=us:2ps:3gl:firmfy23:eng:greendot:090822:nonem:na:Vdi9woAA:1283828067:617702579742:e:Brand_Recruiting-GPS:Brand_Recruiting-GPS-General_Exact:br&pcridmt=617702579742&slid=&gclid=CjwKCAjwiOCgBhAgEiwAjv5whHk28MVGO6D2HMZ0BsHHCSmNOkD22lve3dwTVYajpPSPAHCNGKx9FRoCkykQAvD_BwE&pmtmt=e&mkwid=sVdi9woAA_dc&pkw=deloitte%20gps

Gray, S. (2022, July 21). The Bipartisan House Privacy Bill Would Surpass State Protections. Retrieved February 26, 2023, from Lawfare website: https://www.lawfareblog.com/bipartisan-house-privacy-bill-would-surpass-state-protections

Guidance on Vermont's Act 171 of 2018 Data Broker Regulation. (2018). In Vermont Office of the Attorney General (pp. 1–28). Retrieved from https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf

Gu, K. (2022, September 29). The Fourth Amendment and the Post-Roe Future of Privacy. Retrieved March 15, 2023, from Bill of Health website: https://blog.petrieflom.law.harvard.edu/2022/09/29/the-fourth-amendment-and-the-post-roe-future-of-privacy/

Hendrix, J. (2022, July 24). The Sunday Show: Prospects for the American Data Privacy and Protection Act. Retrieved September 7, 2022, from Tech Policy Press website: https://techpolicy.press/the-sunday-show-prospects-for-the-american-data-privacy-and-protection-act/

Hillier, W. (2022, December 19). The Best Guide To Predictive vs. Prescriptive Analytics. Retrieved October 6, 2022, from CareerFoundry website: https://careerfoundry.com/en/blog/data-analytics/predictive-vs-prescriptive-analytics/

References

House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill. (2022, June 3). Retrieved September 7, 2022, from U.S. Senate Committee on Commerce, Science, & Transportation website: https://www.commerce.senate.gov/2022/6/house-and-senate-leaders-release-bipartisan-discussion-draft-of-comprehensive-data-privacy-bill

How Long Will It Take For My Case to Go to Trial? — McKinney Law Firm. (2022). Retrieved March 12, 2023, from The McKinney Law Firm, P.C. website: https://www.themckinneylawfirm.com/how-long-does-it-take-to-get-a-case-to-trial#:~:text=In%20federal%20court%20it%20is

Ikemura, A. (2010). Home Experian Key Findings Profile Report Benefits Explanation of Terms. In *Experian*. Experian. Retrieved from Experian website: https://www.experian.com/assets/data-university/mosaic-seg-sample-report.pdf

Information Commissioners Office. (n.d.). The Principles: At a Glance. Retrieved from Ico.org.uk website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Jia, J., Jin, G. Z., & Wagman, L. (2018). The Short-Run Effects of GDPR on Technology Venture Investment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3278912

Jones, A. (2021, May 14). GDPR Three Years Later: What Impact Has It Made? Retrieved August 8, 2022, from https://www.ispartnersllc.com/blog/gdpr-one-year-later-impact/

Jukam, T. (2010). Litigation Cost Survey of Major Companies. In *U.S. Chamber Institute for Legal Reform* (pp. 3–34). Retrieved from https://www.uscourts.gov/sites/default/files/litigation_cost_survey_of_major_companies_0.pdf

Jurcys, P. (2019, September 5). What is the Value of Your Data? Retrieved April 10, 2023, from Medium website: https://towardsdatascience.com/what-is-the-value-of-your-data-9341cd019b4d

Kabaria, A., & Seiver, J. (2022, January 13). Illinois “Protecting Household Privacy Act” Takes Effect | Davis Wright Tremaine. Retrieved June 7, 2022, from Davis Wreight Tremaine LLP website: https://www.dwt.com/blogs/privacy--security-law-blog/2022/01/illinois-protecting-household-privacy-act#:~:text=Overview

Kagubare, I., & Klar, R. (2023, February 28). House to tackle data privacy in renewed federal effort. Retrieved February 3, 2023, from The Hill website: https://thehill.com/newsletters/technology/3878109-house-to-tackle-data-privacy-in-renewed-federal-effort/

Katsaros, A., & Khan, L. (2022). Federal Trade Commission Fiscal Year 2023 Congressional Budget Justification. In FTC.gov (pp. 5–74). Washington, D.C. Retrieved from https://chrome-extension ://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf

Keegan, J., & Ng, A. (2021, December 6). The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users – The Markup. Retrieved November 6, 2022, from The Markup website: https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user

Koebler, J., & Merlan, A. (2022, August 9). This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion. Retrieved March 15, 2023, from www.vice.com website: https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion?utm_source=motherboard_twitter

Lavelle, J. (2019, October 2). Gartner Says Robotic Process Automation Can Save Finance Departments 25,000 Hours of Avoidable Work Annually. Retrieved February 23, 2023, from Gartner Newsroom website: https://www.gartner.com/en/newsroom/press-releases/2019-10-02-gartner-says-robotic-process-automation-can-save-fina

Law, R. (2019, May 28). Churn Rate: How High is Too High? A Meta-Analysis of Churn Studies. Retrieved February 18, 2023, from Cobloom.com website: https://www.cobloom.com/blog/churn-rate-how-high-is-too-high

References

Lawrence, D. (2016, April 25). A Leak Wounded This Company. Fighting the Feds Finished It Off. *Bloomberg News*. Retrieved from https://www.bloomberg.com/features/2016-labmd-ftc-tiversa

Legal acts – statistics. (2023). Retrieved April 7, 2023, from eur-lex.europa.eu website: https://eur-lex.europa.eu/statistics/2018/legislative-acts-statistics.html

Lima, C. (2022, June 22). Top Senate Democrat casts doubt on prospect of major data privacy bill. Retrieved February 26, 2023, from The Washington Post website: https://www.washingtonpost.com/technology/2022/06/22/privacy-bill-maria-cantwell-congress/

Lund, S., & al, et. (2013). Game changers: Five opportunities for US growth and renewal. In *McKinsey Global Institute*. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Americas/US%20game%20changers/MGI_Game_changers_US_growth_and_renewal_Full_report.ashx

Lupton, D. (2019). "The Internet Both Reassures and Terrifies": exploring the more-than-human worlds of health information using the story completion method. *Medical Humanities*, *47*, medhum-2019-011700. ResearchGate. https://doi.org/10.1136/medhum-2019-011700

Madden, M. (2014, November 12). Privacy Perceptions. Retrieved March 1, 2023, from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2014/11/12/privacy-perceptions/

Manikya, J. (2013, October). Open data: Unlocking innovation and performance with liquid information | McKinsey. Retrieved March 2, 2023, from www.mckinsey.com website: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

.

Marchsteiner, K. (2021). Strategies for Identifying Reporting Requirements and Submitted Reporting to Congress. In *Congressional Research Service* (pp. 1–14). Washington, D.C. Retrieved from https://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sgp.fas.org/crs/misc/R46661.pdf

Mazanec, M. (2021). *Fiscal Year 2021 Annual Report* (pp. 10–61). Washington, D.C.: Congressional Research Service; Library of Congress.

McGill, M. H., & Fried, I. (2022, June 28). As states outlaw abortion, tech companies will likely hand over user data. Retrieved January 7, 2023, from Axios website: https://www.axios.com/2022/06/28/tech-companies-surrender-abortion-related-data

McKeever, B. (2019, July 23). The Nonprofit Sector in Brief. Retrieved March 1, 2023, from National Center for Charitable Statistics website: https://nccsurban.org/project/nonprofit-sector-brief

McQuinn, A., & Castro, D. (2019, August 5). The Costs of an Unnecessarily Stringent Federal Data Privacy Law. Retrieved March 2, 2023, from Information Technology and Innovation Foundation website: https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/

Medication Abortion. (2016, March 14). Retrieved March 6, 2023, from The Guttmacher Institute website: https://www.guttmacher.org/state-policy/explore/medication-abortion?gclid=Cj0KCQjw27mhBhC9ARIsAIFsETE43p21JotliWSpzz2HY7PNGjEJXadH0mEbHgoD3dEq_8aWVOcBsU4aAkSBEALw_wcB

Michalsons. (2015). Protection of Personal Information Act Summary | POPIA. Retrieved January 6, 2023, from Michalsons website: https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia

References

Morrison, S. (2020, December 2). A surprising number of government agencies buy cellphone location data. Lawmakers want to know why. Retrieved March 1, 2023, from Vox website: https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel

Morrison, S. (2022, July 6). Should I delete my period app? And other post-Roe privacy questions. Retrieved from Vox website: https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion

Murnane, K. (2016, April 11). How Men And Women Differ In Their Approach To Online Privacy And Security. Retrieved March 1, 2023, from Forbes website: https://www.forbes.com/sites/kevinmurnane/2016/04/11/how-men-and-women-differ-in-their-approach-to-online-privacy-and-security/?sh=38b5e3bf7d88

Nagle, T., Redman, T. C., & Sammon, D. (2017, September 11). Only 3% of Companies' Data Meets Basic Quality Standards. Retrieved February 18, 2023, from Harvard Business Review website: https://hbr.org/2017/09/only-3-of-companies-data-meets-basic-quality-standards.

National Museum of American History. (2020, March 2). The Women's March, 2017. Retrieved March 2, 2023, from National Museum of American History website: https://americanhistory.si.edu/creating-icons/women%E2%80%99s-march-2017

New York Times Company Privacy Policy. (2023, March 16). Retrieved January 6, 2023, from The New York Times website: https://help.nytimes.com/hc/en-us/articles/10940941449492-The-New-York-Times-Company-Privacy-Policy-

O'Brien, M., & Liedtke, M. (2021, June 22). How Big Tech created a data "treasure trove" for police. Retrieved March 9, 2023, from Associated Press News website: https://apnews.com/article/how-big-tech-created-data-treasure-trove-for-police-e8a664c7814cc6dd560ba0e0c435bf90

Office for Civil Rights (OCR). (2009, September 10). The Security Rule. Retrieved from U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/security/index.html

Ohio Credit Union League. (2 C.E.). Letter to Consumer Financial Protection Bureau: Request for Information Regarding Consumers' Experience with Free Access to Credit Scores Docket.

Oliver, J. (2022, April 10). Data Brokers: Last Week Tonight with John Oliver (HBO). Retrieved April 11, 2022, from YouTube website: https://www.youtube.com/watch?v=wqn3gR1WTcA

Oster, R. (2023, March 2). Intimate privacy: the fight for cyber civil rights. Retrieved March 3, 2023, from Virginia's Public Media website: https://www.vpm.org/news/2023-03-02/intimate-privacy-digital-period-tracking

Our Feminist Future - Women's March. (2017). Retrieved March 2, 2023, from Women's March website: https://www.womensmarch.com/

Overview of The Privacy Act of 1974 (2020 Edition). (2020, October 14). Retrieved from www.justice.gov website: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

Peterson, J. (2023, March 8). ARC Launch Announcement. Retrieved March 12, 2023, from The Alliance for Responsible Citizenship (ARC) website: https://www.arcforum.com/ideas/the-launch-of-arc/

Pew Research Center. (2019, June 12). Internet/Broadband Fact Sheet. Retrieved from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Pokora, B., & Perkins-Southam, T. (2023, March 9). Credit Card Statistics And Trends 2023 – Forbes Advisor. Retrieved March 2, 2023, from www.forbes.com website: https://www.forbes.com/advisor/credit-cards/credit-card-statistics/#:~:text=How%20Many%20Credit%20Cards%20Do

References

PREPARED BY: 85% SUCCESS RATE ON LARGE VIABLE CLAIMS 85% BUSINESS CREDIT REPORT SURVEY Share This Ebook! (2015). In The Kaplan Group. Retrieved from https://www.kaplancollectionagency.com/wp-content/uploads/2012/07/Business-Credit-Report-Survey-Version-1.02.pdf

R.E. (2022, November 9). Commercial Surveillance ANPR, R111004; Question 5. Federal Trade Commission.

REPUBLIC OF SOUTH AFRICA. (2013). Government Gazette. In REPUBLIC OF SOUTH AFRICA (pp. 1–76). Cape Town. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, 10(1). https://doi.org/10.1038/s41467-019-10933-3

Rodgers, C. M. (2022, July 20). McMorris Rodgers Leads Group of Bipartisan Leaders to Advance American Data Privacy and Protection Act Through Committee. Retrieved April 7, 2023, from House Representative Cathy McMorris Rodgers website: https://mcmorris.house.gov/posts/mcmorris-rodgers-leads-group-of-bipartisan-leaders-to-advance-american-data-privacy-and-protection-act

Rubio, M. (2019, January 16). Rubio Introduces Privacy Bill to Protect Consumers While Promoting Innovation. Retrieved January 6, 2023, from U.S. Senator for Florida, Marco Rubio website: https://www.rubio.senate.gov/public/index.cfm/2019/1/rubio-introduces-privacy-bill-to-protect-consumers-while-promoting-innovation

Ryan, T. H.R.4346 legislative branch appropriations bill, 2022. , 20 § (2022).

Silverberg, K. (2022, September 30). Business Roundtable Comments on the American Data Privacy and Protection Act. Retrieved February 27, 2023, from The Business Roundtable website: https://www.businessroundtable.org/business-roundtable-comments-on-the-american-data-privacy-and-protection-act

Sterrett, D., & Benz, J. (2021, September 16). Trust in Government is Low, but Americans are United Around Investments in Technology. Retrieved from NORC Center for Public Affairs Research website: https://apnorc.org/projects/trust-in-government-is-low-but-americans-are-united-around-investments-in-technology/

Streim, A., & Weiß, R. (2019, May 16). Annual Survey: Bitkom draws mixed conclusion regarding GDPR implementation | Presseinformation | Bitkom e.V. Retrieved November 7, 2022, from www.bitkom.org website: https://www.bitkom.org/EN/List-and-detailpages/Press/Annual-Survey-Bitkom-draws-mixed-conclusion-regarding-GDPR-implementation

Survey Shows An Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores · Consumer Federation of America. (2018, June 18). Retrieved March 1, 2023, from Consumer Federation of America website: https://consumerfed.org/press_release/survey-shows-an-increasing-number-of-consumers-have-obtained-their-credit-scores-and-know-much-more-about-credit-scores/

Swagel, P. (2022, July 27). The Demographic Outlook: 2022 to 2052 | Congressional Budget Office. Retrieved February 25, 2023, from Congressional Budget Office website: https://www.cbo.gov/publication/57975

The 2020 Mom Policy Team. (n.d.). Federal Policy. Retrieved March 2, 2023, from 2020 Mom website: https://www.2020mom.org/federal-policy-blogs

The European Parliament And The Council Of The European Union. (2016). on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (pp. 1–88). Official Journal of the European Union. Retrieved from Official Journal of the European Union website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

References

The Principles. (2019, January 18). Retrieved from Information Commissioners Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Thibault, D. (2022, June 30). Flo Launches Anonymous Mode. Retrieved from FloHealth website: https://flo.health/press-center/flo-launches-anonymous-mode

Tollet, G. (2021, January 30). Brands face a “year of change” with consumer privacy laws. Retrieved March 15, 2023, from VentureBeat website: https://venturebeat.com/business/brands-face-a-year-of-change-with-consumer-privacy-laws/

Torchinsky, R. (2022, June 24). How period tracking apps and data privacy fit into a post-Roe v. Wade climate. *NPR*. Retrieved from https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps#:~:text=Wade%20climate%20%3A%20NPR&text=Press-

Upholding information rights for all A guide to the legislation the ICO regulates. (2012). In *Information Commissioner’s Office*. United Kingdom. Retrieved from https://ico.org.uk/media/1042840/upholding_information_rights_for_all.pdf

U.S. Census Populations With Bridged Race Categories. (2022, October 28). Retrieved March 1, 2023, from https://www.cdc.gov website: https://www.cdc.gov/nchs/nvss/bridged_race.htm#Newest%20Data%20Release

U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action. (2022, May 31). Retrieved February 26, 2023, from U.S. Chamber of Commerce website: https://www.uschamber.com/technology/data-privacy/u-s-chamber-warns-it-will-oppose-any-privacy-legislation-that-creates-a-blanket-private-right-of-action

U.S. Department of Homeland Security. (2014). IT 20140218 Digital Footprint. In *National Cybersecurity and Communications Integration Center* (pp. 1–14). Washington, D.C. Retrieved from https://www.urmc.rochester.edu/MediaLibraries/URMCMedia/flrtc/documents/IT-20140218_Digital-Footprint.pdf

Van Ooijen, I., & Vrabec, H. U. (2018). Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Warner, M. (2018). Potential Policy Proposals for Regulation of Social Media and Technology Firms. In *Senate.gov* (pp. 1–23). Washington, D.C. Retrieved from https://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf

Wasson, E. (2022, December 22). Congress Clears $1.7 Trillion Funding Bill With Ukraine Aid. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2022-12-22/senate-passes-giant-spending-bill-with-ukraine-aid-election-change

What are cookies? (2018, April 24). Retrieved October 5, 2022, from Kaspersky website: https://www.kaspersky.com/resource-center/definitions/cookies

Wyatt, M., & Citron, D. (2022, September 28). Professor Danielle Citron’s New Book Argues Intimate Privacy Is a Human Right. Retrieved February 6, 2023, from University of Virginia School of Law website: https://www.law.virginia.edu/news/202209/professor-danielle-citrons-new-book-argues-intimate-privacy-human-right

Appendix

Table A

Data Privacy Bill of Rights Costing

Table	Cost Category	Cost Type	Cost	Sources
B	Compliance	Compliance Personnel	$6,370M	(McQuinn & Castro, 2019); (Country Business Patterns: 2020 SUSB Annual Data Tables by Establishment Industry, 2020); (McKeever, 2019); (Data Analyst Salaries, 2023)
C	Compliance	Privacy Audits	$440M	(McQuinn & Castro, 2019); (Good, 2019)
D	Compliance	Data Infrastructure	$5,380M	(Clement, 2018); (McQuinn & Castro, 2019); (Data Analyst Salaries, 2023); (Nagle et al., 2017)
E	Compliance	Data Access	$274.5M	(McQuinn & Castro, 2019); (Dashlane, 2015); (Letter to Consumer Financial Protection Bureau: Request for Information Regarding Consumers' Experience with Free Access to Credit Scores Docket, 2 C.E.)
F	Compliance	Data Opt-Out	$340M	(McQuinn & Castro, 2019); ("Data Sharing and Open Data for Banks a Report for HM Treasury and Cabinet Office Data Sharing and Open Data for Banks --A Report for HM Treasury and Cabinet Office," 2014)
G	Compliance	Data Deletion	$780M	(Law, 2019); (McQuinn & Castro, 2019)
H	Compliance	Data Rectification	$55.35M	(Survey Shows an Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More about Credit Scores · Consumer Federation of America, 2018); (McQuinn & Castro, 2019); (Google Transparency Report, 2019); (Pokora & Perkins-Southam, 2023)
I	Market Inefficiency	Less Access to Data	$71,000M	(Lund & al, 2013); (McQuinn & Castro, 2019); (Manikya, 2013)
J	Market Inefficiency	Lower Ad Effectiveness	$8,000M	(Deighton & Johnson, 2015); (Goldfarb & Tucker, 2011); (McQuinn & Castro, 2019)
Total Excluding PRA			**$92,640M**	
K	Compliance	Private Right to Action	$2,710M	(Lawrence, 2016); (McQuinn & Castro, 2019); (Jukam, 2010); (Brown, 2019)
Total Including PRA			**$95,350M**	

Table B

Privacy Personnel Costing

Data privacy laws necessitates hiring new compliance personnel (CPs) to manage user privacy requests, system upkeep, and regulatory compliance. Current personnel must divert energy and time away from other obligations to accommodate new responsibilities. The total annual cost of hiring and maintaining privacy personnel will be $6.37 billion

Type of Organization	# of CPs	$ per CP	Cost
Small Business	26,000	$108,000	$2,180M
Medium Business	15,000	$108,000	$1,620M
Large Business	10,000	$108,000	$1,080M
Nonprofit	8,000	$108,000	$860M
Total Cost			**$6,370M**

Assumptions

There are ~53,000 small businesses, 616,000 medium-sized businesses, and 19,000 large business in the U.S. according to the U.S. Census Bureau. The ITIF finds that across these companies, 51,000 new compliance officers will have to be hired.

The National Center for Charitable Statistics suggests a need for an additional 8,000 officers for the 1.56 million existing American nonprofits.

According to Glassdoor, the average annual salary of privacy officers is $77,000.

The ITIF finds adding costs for employee benefits, paying taxes, administrative costs, and office space requires using a cost multiplier between 1.4-2.3x per hire.

Using the more expensive end of the multiplier range, the ITIF finds each compliance officer will cost an average of $108,000/year for a total of $6.37 billion in the first year.

Sources

(McQuinn & Castro, 2019); (Country Business Patterns: 2020 SUSB Annual Data Tables by Establishment Industry, 2020); (McKeever, 2019); (Data Analyst Salaries, 2023)

Table C

Audits Costing

Privacy audits are necessary to ensure companies and organizations are handling personal data in compliance with the DPBR.

Type of Organization	# of Audits	$ per Audit	Cost
Small Business	26,000	$10,000	$260M
Medium Business	3,000	$30,000	$90M
Large Business	100	$60,000	$6M
Nonprofit	8,000	$10,000	$80M
Total Cost			**$440M**

Assumptions

We use HIPAA compliance costs as a benchmark. According to the healthcare compliance firm, Datica, HIPAA audits costs range from $10,000 to $60,000 per year depending on the size of the business.

Datica finds that small businesses and nonprofits will have to spend approximately $10,000 per audit, medium sized companies will spend approximately $30,000, large companies will spend an average of $60,000, and nonprofits will spend $10,000 per audit. The total annual cost to accommodate data audits will be $440 million.

Sources

(McQuinn & Castro, 2019); (Good, 2019)

Table D

Data Infrastructure

Collecting data is cheap, but designing and maintaining data infrastructure is not. Meeting data quality standards is complex as company databases often do not communicate across platforms and frequently neglect to flag partial or inadequately-formatted data. The DPBR requires previously amassed data to be properly arranged in the correct format. This requires manpower. Costs will differ between smaller and newer businesses, which can build systems rather than retrofit outmoded infrastructure. Data infrastructure will cost $5.4 billion in the first year.

Type of Organization	# of New Hires	$ per Hire	Cost
Small Business	26,000	$91,000	$2,370M
Medium Business	3,000	$91,000	$1,370M
Large Business	100	$91,000	$910M
Nonprofit	8,000	$91,000	$730M
Total Cost			**$5,380M**

Assumptions

According to Statista, the U.S. has 238 million internet users over 14 years old, and the average U.S. Internet user has 130 online accounts.

One Harvard Business Review report found that of 75 major companies, a mere 3% had data infrastructures that met basic quality standards.

The ITIF estimates 10% of small businesses and nonprofits, 25% of mid-sized businesses, and 50% of large businesses will require an average of 5% more personnel to restructure online infrastructure.

Glassdoor suggests the average salary for new administrators and data analyst staff is $65,000.

The ITIF suggests an overhead cost multiplier of 1.4 given additional responsibilities associated with creating and maintaining a new system, rendering per-hire cost $91,000.

Sources

(Clement, 2018); (McQuinn & Castro, 2019); (Data Analyst Salaries, 2023); (Nagle et al., 2017)

Table E

Data Access Costing

To estimate the cost of the right to be informed, we extrapolate information gleaned since the E.U.'s GDPR was enacted. The total annual cost for data access is $274.5 billion.

Description	# of Requests	$ per Request	Cost
Verifying Low Impact Requests	290,000,000	$0.15	$43,500,000
Verifying High Impact Requests	375,000,000	$0.25	$93,750,000
Processing Low Impact Requests	290,000,000	$0.15	$43,500,000
Processing High Impact Requests	375,000,000	$0.25	$93,750,000
Total Cost			**$274.5M**

Assumptions

American consumers have 31 billion online accounts, but some are more likely to elicit access requests, including financial and healthcare services. These high-impact online services account for about 5% of all online accounts, or 1.5 billion accounts.

The ITIF reports that since GDPR took effect, about 25% of consumers made requests for these accounts. 25% of 1.5 billion accounts is roughly 375,000,000 requests.

Low-impact services, such as streaming services (of which there are 29 billion accounts) are expected to elicit some requests. According to the ITIF, approximately 1% of those accounts elicit requests, which in the U.S. would be approximately 290 thousand requests per year.

Using credit score reporting to extrapolate the price per request, the Ohio Credit Union League estimates FICO-score release costs between 5-15 cents each. We will use the higher price for a more holistic account of low-impact request costs. The number and complexity of high-impact requests are estimated by the ITIF to be 25 cents per request.

According to the ITIF, the cost for processing and verification of requests is roughly equal.

Sources

(McQuinn & Castro, 2019); (Dashlane, 2015); (Letter to Consumer Financial Protection Bureau: Request for Information Regarding Consumers' Experience with Free Access to Credit Scores Docket, 2 C.E.)

Table F

Data Opt-Out Costing

Costs for processing are expected to be higher depending on the particular needs of the business. The total annual cost for data opt-out is $340 million.

Description	# of Requests	$ per Request	Cost
Verification	680M	$0.25	$170M
Processing	680M	$0.25	$170M
Total Cost			**$340M**

Assumptions

The infrastructure required to verify opting out of data collection is virtually identical to that of data access. As such, the cost per verification request is 25 cents. Given the ITIF's estimated 680 million opt-out requests, the costs associated with verifying users would be $170 million annually.

The ITIF estimates processing the average opt-out request will cost around 25 cents each. Assuming about 680 million requests, processing costs will be about $170 million annually.

Sources

(McQuinn & Castro, 2019); (“Data Sharing and Open Data for Banks a Report for HM Treasury and Cabinet Office Data Sharing and Open Data for Banks --A Report for HM Treasury and Cabinet Office,” 2014)

Table G

Data Deletion Costing

Of the 31 billion accounts in the U.S., 1.5 billion deletion requests are expected. The total cost of deletion requests will be $780 million each year.

Description	# of Requests	$ per Request	Cost
Verification	1,550M	$0.25	$380M
Processing	1,550M	$0.25	$390M
Total Cost			**$780M**

Assumptions

One CoBloom metanalysis reveals that 44% of startups self-reported a "churn rate" (i.e., the rates of attrition of customers from services) of 3-7%, while 30% reported churn rates over 15%.

The ITIF recommends using a 5% churn rate to balance estimates.

The ITIF estimates cost to verify and process request is 25 cents, as infrastructure for deletion is identical to that of opting out.

The ITIF estimates 1.55 billion deletion requests each year.

Sources

(Law, 2019); (McQuinn & Castro, 2019)

Table H

Data Rectification Costing

The annual cost for data rectification is $55.35 million.

Description	# of Requests	$ per Request	Cost
Verifying Low Impact Requests	29,000,000	$0.25	$7,250,000
Verifying High Impact Requests	15,280,000	$0.25	$3,820,000
Processing Low Impact Requests	29,000,000	$1	$29,000,000
Processing High Impact Requests	15,280,000	$1	$15,280,000
Total Cost			**$55,350,000**

Assumptions

According to the Consumer Federation of America, 8% of American consumers currently seek to correct their credit reports. We will use this request rate to extrapolate general high-impact account rectification requests. According to Forbes, 191 million Americans have credit cards, this will lead to 15,280,000 requests each year.

For low-impact online activities, we extrapolate using Google's adherence to the GDPR's "right to be forgotten", which has generated 29 million requests on an annual basis.

The ITIF finds that this represents 0.1% of all low-impact accounts, which of 29 billion accounts in the U.S. would mean we expect which in the U.S. would lead to roughly 29 million correction requests annually.

Verifying these requests utilizes the same infrastructure and personnel that data access requires. As such, the price per request will be 25 cents.

Processing requests requires an additional mechanism to correct information after it has been requested for deletion. The ITIF estimates the average cost will be $1 per request.

Sources

(Survey Shows an Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More about Credit Scores · Consumer Federation of America, 2018); (McQuinn & Castro, 2019); (Google Transparency Report, 2019); (Pokora & Perkins-Southam, 2023)

Table I

Reduced Access to Data

Data privacy requirements for express consent, data minimization, or purpose specification may reduce data access, limit data sharing, ultimately hamper innovation. It's possible such restrictions will hamper automation, optimizing commercial productivity, and identifying new customers.

***Assumptions*:**

1. McKinsey Global Institute highlights multiple "game changing" arenas where improved access and data processing could generate billions for the American economy and create jobs, primarily in the data analytics fields. According to that report, the U.S. would have enjoyed a $1.3 trillion dollar benefit if they expanded data sharing in the private sector.
2. This bill would, according to McKinsey, cause a 5% loss in the current value of data. Given the current size of the data analytics market, McKinsey expects a **$71bn hit to the economy.**

Sources:
(Lund & al, 2013); (McQuinn & Castro, 2019); (Manikya & al, 2013)

Table J

Lower Ad Effectiveness

Many companies collect and sell their user's data to data brokers to enable other companies to target advertising to individuals who may be likely to purchase their products or services. When companies can no longer buy this data freely, they cannot target potential buyers as efficiently, and their ability to gage the effectiveness of certain advertising methods is also reduced.

***Assumptions*:**

1. According to one Management Science study, restrictive EU rules initiated an average drop in the effectiveness of online ads by approximately 5% in first-party advertising and a 10% dip in third-party advertising.
2. Changes in federal regulation would impact third-party ads (whose business nearly exclusively relies on cookies) more than first-party ads. Goldfarb and Tucker estimate a national decline of 8%, or approximately **$8 billion, in total lost advertising revenues**.

Sources:
(Deighton & Johnson, 2015); (Goldfarb & Tucker, 2011); (McQuinn & Castro, 2019)

Table K

Private Right to Action Costing

Lawyer and court fees associated with defending lawsuits may be exacerbated by the potential for frivolous lawsuits. Given the following parameters, the PRA may lead to an additional $2.7 billion hit to the economy each year.

Description	# of Suits	$ per Suits	Cost
Federal Lawsuits	10	$1,000,000	$10M
State Lawsuits	200	$1,000,000	$200M
Class Action Lawsuits	50	$50,000,000	$2,500M
Total Cost			**$2,710,000**

Assumptions

One study completed by the House Oversight Committee found the average annual cost of fighting lawsuits--even those that are thrown out--is $1 million in attorney's fees.

ITIF research finds that states may bring 400 lawsuits each year while there may be 20 federal lawsuits. Of these, approximately 50% are expected to be dropped. Therefore, 200 state lawsuits and 10 federal lawsuits are expected to stand.

ITIF research suggests that federal class actions for consumer protection statutes are 6x more likely to occur in federal courts, resulting in 100 lawsuits, of which they approximate 50 will be dismissed.

The ITIF's conservative estimate for class-action lawsuits following the PRA would cost organizations roughly $50 million dollars each.

Sources

(Lawrence, 2016); (McQuinn & Castro, 2019); (Jukam, 2010); (Brown, 2019)