Seattle Journal of Technology, Environmental & Innovation Law

Volume 14
Issue 2 *Volume 14 Issue 2*

Article 3

5-18-2024

All in the Name of Safety: Abortion and Gun Control Purchase Monitoring Create a Call for Stricter Data Privacy Regulation in Financial Institutions

Emilee Crapo
rizzok@seattleu.edu

All in the Name of Safety: Abortion and Gun Control Purchase Monitoring Create a Call for Stricter Data Privacy Regulation in Financial Institutions

Emilee Crapo

Table of Contents

I. INTRODUCTION

The increased technology developments have provided many great advancements that have aided developments in healthcare, education, business, and much more. Yet these advancements have added greater concerns to data privacy. It has raised concerns about what information corporations should be allowed to access, what type of information is shared, and the government's overall role in holding these entities responsible.

Specifically, beginning in June 2022, with the overturning of *Roe v. Wade*, concerns began intensifying over the possibility of financial data being used as evidence for abortion investigations.[1] A couple of months later, this concern spread even further with lawmakers pushing credit card companies to begin tracking gun shops to monitor firearm purchases.[2] This has stimulated conversations filled with a growing concern around data privacy within these financial institutions. The current regulations imposed throughout the United States are broad. As technology continues to grow, advance, and infiltrate every aspect of American life, it begs the question of what it would look like to enforce stricter data privacy regulations when it comes to the relationship of consumer spending and financial companies.

While financial institutions claim their needs to report on potentially dangerous consumer spending, there should be stricter federal data privacy regulations when it comes to the monitoring because consumers have a right to privacy and a right to spend their money how they choose. Stricter regulation would also increase confidence in government and financial institutions. Some areas of privacy that should be addressed within a federal data privacy law would include: (1) creating greater incentives and penalties for corporations to comply and encouraging entities to think more strategically regarding the way they target consumer data; (2) building upon state regulations instead of imposing a ceiling that is limiting; and (3) a stronger enforcement of transparency in the relationship between data holders and consumers.

This paper will discuss the history of data privacy in the United States, specifically in relation to financial organizations. Then, it will analyze the different monitoring methods that create concerns for consumers to the monitoring of purchases at firearm stores and abortion clinics. Finally, it will analyze how these methods are causes for concern and ultimately point to the substantial need for a federal data privacy law in the United States.

---

[1] Ron Lieber and Tara Siegel Bernard, *Payment Data Could Become Evidence of Abortion, Now Illegal in Some States*, NEW YORK TIMES (June 29, 2022) https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html [https://perma.cc/55ZE-H7CX].

[2] AnnaMaria Andriotis, *Visa, Mastercard, Amex to Track Gun Shops with New Merchant Code*, WALL ST. J. (Sept. 11, 2022), https://www.wsj.com/articles/visa-mastercard-amex-to-track-gun-shops-with-new-merchant-code-11662915056?mod=Searchresults_pos1&page=1 [https://perma.cc/P5Z4-YVPF].

II. HISTORY OF DATA PRIVACY

The Fourth Amendment protects an individual's right "against unreasonable searches and seizures,"[3] which applies "every time government officials (not just police) conduct a 'search' or 'seizure' of an object, document, or person."[4] This has been the strongest authority in privacy protection but does contain a significant caveat known as the third-party doctrine. This doctrine states that "a person has no legitimate expectation of privacy in information [they] voluntarily turn over to third parties."[5] When a consumer agrees to a company's privacy policy, the third-party doctrine is invoked, and they forfeit the Fourth Amendment protection of their data. This has created an interesting relationship between the third-party doctrine and privacy policies that have left consumers' privacy more often in the hands of major corporations than the government. Several commissions and regulations have been put in place over the years to protect and secure consumer data information. Specifically, for financial information, the critical regulations are found with the Federal Trade Commission (FTC), the Gramm-Leach-Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA).

A. Federal Trade Commission

Created in 1914, the Federal Trade Commission was established to work to prevent fraud, as well as deceptive and unfair business practices.[6] The commission connects with consumers by providing information to help them spot and avoid scams and fraud.[7] The ultimate goals of the FTC are to prevent unfair and deceptive practices; prevent unfair methods of competition; and advance performance through resources, human capital, and information technology.[8] Ultimately, Congress decided that the FTC would enforce privacy promises under its watch.[9] The FTC would include four major sectors where federal law would regulate privacy policies which would include: children under the age of thirteen covered by the Children's Online Privacy Protection Act of 1998 (COPPA), financial institutions covered by the GLBA, health care providers covered by the Health Insurance Portability and

---

[3] U.S. CONST. amend. IV.
[4] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 270 (Wolters Kluwer, 7th ed. 2021).
[5] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).
[6] *Federal Trade Commission*, USAGOV, https://www.usa.gov/federal-agencies/federal-trade-commission, [https://perma.cc/3JVM-ERAS] (last visited Mar. 22, 2024).
[7] *Id.*
[8] *About the FTC*, FEDERAL TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/BVH4-ZR89] (last visited Mar. 10, 2024).
[9] Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 73 (2007).

Accountability Act of 1996 (HIPAA), and federal government agencies covered by the E-Government Act of 2002 (EGA).[10]

Even though the FTC continues to be the sole power regulating privacy and its enforcement, regulators and privacy professionals have confronted the FTC for unfair and deceptive practices.[11] This is largely due to investigations against institutions completed by the FTC for privacy violations. It has been routinely held that companies that seems to exploit a consumer's personal information may continue to do so if it can prove that it put consumers on notice that this collection of data would happen. [12] The FTC criticism spans far and wide, but it could hold the key to the implementation of a federal privacy law, as many technology companies are willing to spend copious amounts of money to block regulation imposed by Congress.[13] Rulemaking by the FTC is incredibly burdensome and rarely done but seeing as technological institutions have spent over $100 million to block privacy regulation in Congress, it could be argued that the burden has shifted to the FTC to lead expansions in privacy law.[14]

B. Fair Credit Reporting Act

The Fair Credit Reporting Act was enacted in 1970 to promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies (CRA).[15] This was the first federal law passed to regulate the use of personal information by private businesses.[16] The late 1960s brought a lot of abuse in the industry of using "lifestyle" information such as sexual orientation, marital status, drinking habits, and cleanliness.[17] The increased public exposure created a demand for Congressional inquiry and federal regulation of CRAs.[18]

CRAs will produce reports on individuals for businesses—including credit card companies, banks, employers, landlords, and others.[19] This complex statute has been revised significantly since 1970, but the main purpose remains to require that CRAs follow "reasonable procedures" to protect the confidentiality, accuracy, and relevance of credit

---

[10] *Id*. at 74.
[11] *See* Jordan Crenshaw, *Why Recent FTC Privacy Actions Signal Need for Congress to Rein in the Commission*, U.S. CHAMBER OF COM. (May 16, 2023), https://www.uschamber.com/technology/data-privacy/why-recent-ftc-privacy-actions-signal-need-for-congress-to-rein-in-the-commission [https://perma.cc/MK2Z-CM9N].
[12] Courtney C. Seitz, *The Third-Party Doctrine: Perpetuation by Privacy Policies*, 34 NOTRE DAME J.L ETHICS & PUB. POL'Y 421, 436 (2020).
[13] John D. McKinnon & Chad Day, *Tech Companies Make Final Push to Head Off Tougher Regulation*, WALL ST. J. (Dec. 19, 2022), https://www.wsj.com/articles/tech-companies-make-final-push-to-head-off-tougher-regulation-11671401283?mod=article_inline [https://perma.cc/32WF-YKVH].
[14] *Id*.
[15] *The Fair Credit Reporting Act (FCRA)*, ELEC. PRIV. INFO. CTR., https://epic.org/fcra/#:~:text=The%20Fair%20Credit%20Reporting%20Act%20(FCRA)%2C%20Public%20Law%20No,Credit%20Reporting%20Agencies%20(CRAs) [https://perma.cc/2AXZ-8QSG] (last visited Mar. 8, 2024) [hereinafter "FCRA"].
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id*.

information.[20] A CRA is an entity that assembles and sells credit and financial information about individuals.[21] This can include one of the three national CRAs:[22] a smaller credit reporting agency; inspection bureaus; and depending on the nature of the operation, detective agencies.[23]

This statute has developed considerably since its inception, including law enforcement's broadened access through the USA PATRIOT Act and the Fair and Accurate Credit Transactions amendments.[24] The most recent changes imposed in 2021 include consumers having the right to restrict a person from using certain information obtained from an affiliate to make solicitations to the consumer, requirements of accuracy and integrity by those entities providing consumer information to CRAs, and providing consumers with notice that their information from a consumer report is being used for less than favorable terms.[25]

C. Gramm-Leach-Bliley Act

Passed in 1999, the Gramm-Leach-Bliley Act required financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.[26] The act provides specific definitions of what constitutes nonpublic personal, customer, and financial information.[27]

Under the GLBA, nonpublic personal information includes personally identifiable financial information, as well as any list, description, or other grouping of consumers that is derived using this specific information.[28] Customer information is any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled by the institution.[29] A financial institution is a business that engages in financial activity. [30]

---

[20] *Id.*
[21] *Id.*
[22] This includes Equifax, TransUnion, and Experian.
[23] FRCA, *supra* note 15.
[24] *Id.*
[25] *FTC Approves Changes to Five FCRA Rules*, FEDERAL TRADE COMMISSION: PROTECTING AMERICA'S CONSUMERS (September 8, 2021) https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-approves-changes-five-fcra-rules [https://perma.cc/D3PG-RY8V].
[26] *Gramm-Leach-Bliley Act*, FEDERAL TRADE COMM'N PROTECTING AMERICA'S CONSUMERS, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act [https://perma.cc/Q44G-FZMF] (last visited Mar. 10, 2024).
[27] *FTC Safeguards Rule: What your Business Needs to Know*, FEDERAL TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know#Information_security_program [https://perma.cc/LHN8-7JSY] (last visited Apr. 2, 2024).
[28] 16 C.F.R. § 314.2(l)(1) (2014).
[29] 16 C.F.R. § 314.2(d) (2014).
[30] 16 C.F.R. § 314.2(h)(1) (2014).

Under the GLBA, privacy includes ensuring the security and confidentiality of customer information, as well as protecting against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer.[31] It prohibits financial institutions from disclosing a consumer's financial information to third parties without first notifying the consumer.[32] The act also requires institutions to protect against anticipated threats or hazards to the security or integrity of such information.[33] Banks, savings and loans companies, credit unions, insurance companies and securities firms could accomplish this by allowing consumers to opt out of sharing information.[34] This provides information to the consumer by disclosing how each of these institutions will protect confidentiality and security of their information.[35]

However, the GLBA still allows companies to sell customer's financial data to anyone they choose—including credit card information––unless the customer takes affirmative action.[36] This would include an opt-out option that must be repeated for each financial institution. Some have said this feels like pulling teeth with credit card companies.[37] The information that a company could access includes the date of the purchase, amount, recipient of the charges, and the personal details that are included in credit card applications.[38] While the GLBA does require financial institutions to inform their customers about the information that is being used, the information does not have to be clear and easy to find but can be hidden in the fine print of a user agreement.[39]

Whilst each of the aforementioned entities and regulations do impose restrictions on invading a consumer's privacy, many working in constructing privacy policies have turned to the European Union, which has seemingly become the ultimate authority in privacy regulation.

III. EUROPEAN UNION'S PRIVACY LAWS AND ITS IMPACT ON THE PRIVACY CONVERSATION IN THE UNITED STATES

[31] *Privacy Act Issues under Gramm-Leach-Bliley*, FED. DEPOSIT INS. CORP. (Sept. 14, 2022), https://www.fdic.gov/consumers/consumer/alerts/glba.html [https://perma.cc/Y3XJ-H7U2] (hereinafter "Issues under GLB").
[32] CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 3 (2022).
[33] Issues under GLB, *supra* note 31.
[34] *Id.*
[35] *Id*.
[36] Jay Stanley, *Why Don't We Have More Privacy When We Use A Credit Card?,* AM. C.L. UNION (Aug. 13, 2019), https://www.aclu.org/news/privacy-technology/why-dont-we-have-more-privacy-when-we-use-credit-card [https://perma.cc/4TKT-H6J3].
[37] *Id*.
[38] *Id*.
[39] *Id*.

In May 2018, the European Union (E.U.) passed the toughest privacy and security law in the world.[40] Though drafted and passed in the E.U., the General Data Protection Regulation (GDPR) imposes obligations onto organizations anywhere, so long as they target data related to people in the E.U.[41]

A. Implementation and Obligations under the GDPR

The implementation of the GDPR signals a shift in the conversation regarding data privacy, not just in Europe, but throughout the world.[42] Europe is taking a firm stance on data privacy and security at a time when more and more people are entrusting their personal data with cloud services and breaches are becoming a daily occurrence.[43] The regulation is large, far-reaching, and light on specifics, making it daunting for most corporations, specifically small and medium-sized businesses.[44] The specific toughness of the GDPR stems from the minimum eight-figure fine imposed if the regulation is violated, as well as requiring entities to create both internal and external mechanisms to augment enforcement efforts.[45] In the development of the GDPR, European policy makers gathered experts in the field about how information practices should be implemented.[46]

So, the experts created several strategic implications that the GDPR would impose. First, the regulation would encourage companies to think carefully about consumer data and plan for the collection, use and destruction of what is collected.[47] Next, it would deter executives from overlooking data protections by imposing monetary penalties, expanding security incident notifications, and improving procedural requirements.[48] It would also require contractual commitments on data use, security, breach notification, and data retention in order to use data.[49] Next, the regulation would require the use of a Data Protection Officer to be present and monitor companies that offer tenure—like rights.[50] Also, it would treat consumer consent on par with medical consent, which is notably the highest form of consent prior to implementation of the

---

[40] *What is the GDPR, the EU's new data protection law?,* GDPR.EU, https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU [https://perma.cc/83K5-Z62B] (last visited Apr. 2, 2024).
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] Chris Jay Hoofnagle Et Al., *The European Union general data protection regulation: what it is and what it means*, INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 28:1, 66 (2019).
[46] *Id*. at 71.
[47] *Id*. at 67.
[48] *Id*. at 68.
[49] *Id*.
[50] *Id*.

GDPR.[51] This would make it almost impossible to share data legally, as most of the rules imposed are not waivable.[52] Finally, the regulation goes beyond first-party relationships by creating incentives and invoking further burdens on third-party relationships and data sharing between parties.[53]

The E.U. recognizes the difficulty of a complete bar of all data that is used and shared among corporations.[54] So, the regulation imposes a balancing test regarding legitimate interests.[55] The legitimate interest test recognizes situations where "such interests are overridden by the interests or fundamental rights and freedom of the data subject which require protection of personal data."[56] For example, a technology company can store a consumer's Internal Protocol (IP) address for a certain amount of time for security or fraud prevention, but it must be explicitly disclosed to the consumer.[57]

While these are strong incentives and guidelines within the E.U., these rules extend far beyond Europe. If data is to be transferred outside the E.U., it must be explicitly approved by an adequacy decision led by the European Commission.[58] If a country does not get approval, it can still access data but only by contractually agreeing to uphold the level of data protection that is similar to what is set out in the GDPR.[59] For example, after facing many legal challenges, the E.U. and U.S. recently adopted an adequacy decision referred to as the E.U.-U.S. Data Privacy Framework.[60] This decision ensures U.S. protection of personal data transferred between countries is comparable to that offered in the E.U.[61] However, the data protection relationship between the U.S. and E.U. has historically been an issue due to the U.S. not adopting privacy rules that comply with adequacy status.[62] The privacy shield was struck down in 2020 through the *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* case due to its inability to protect data subjects' personal information from the U.S. government, whose powers under limited surveillance laws reach this data.[63] Under this new decision, the U.S. has implemented unprecedented commitments that include providing protections essentially equivalent to those laid out in

---

[51] *Id*. at 68.
[52] *Id*.
[53] *Id*.
[54] *Id*. at 81.
[55] *Id*.
[56] GDPR § 6(1)(f) (2018).
[57] *Id*.
[58] Hoofnagle Et Al., *supra* note 45, at 84.
[59] *Id*.
[60] Jennifer Bryant, *European Commission Adopts EU-US Adequacy Decision*, IAPP (Jul. 10, 2023), https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/ [https://perma.cc/5ZD5-PAPD] (last visited Apr. 2, 2024) (hereinafter "EU-US Adequacy Decision").
[61] *Id*.
[62] Hoofnagle Et Al., *supra* note 45, at 84.
[63] Robert Bateman, *Why the EU-U.S. Privacy Shield was Invalidated*, TERMSFEED, https://www.termsfeed.com/blog/why-eu-us-privacy-shield-invalidated/#Analysis_Of_Schrems_Ii [https://perma.cc/AM97-LFME] (last visited Apr. 2, 2024, 2:58 pm).

E.U. law.[64] Even if this adequacy decision is substantially different than past privacy shields, there is still concern that it will withstand an appeal over the criticism of its "fundamental surveillance issues."[65] The challenge of this framework will take several years, but in the meantime should enable data flows to continue through mechanisms like standard contractual clauses and binding corporate rules.[66] The continued hope is that whatever concerns arise, there will be sufficient space to address them through transparency and mutual understanding, and possibly even policy changes.[67]

B. GDPR Shortcomings

In April of 2022, there was a study conducted to focus on the impact of the GDPR. The study focused on understanding the data holders' compliance with legislation, evaluating data portability, and assessing how the GDPR improves conciseness, fairness, consent, transparency, and reduction of data breach risks.[68] The study was conducted through various interviews with data holders, as well as many requests for how and when their personal information was being used.[69] Ultimately, the study determined that even after the GDPR was enacted, there is still a significant amount of confusing data and insufficient transparency, thus creating fragile relationships between data collectors and consumers.[70]

When requesting the personal data collected, users often received large technical files that were hard to understand and lacked any sort of explanation.[71] The amount of data held by corporations ranged among different entities, but many users were shocked at how much information was being used.[72] The study points out that the relationship between data holders and consumers presents a key dynamic: individuals sacrifice their data in exchange for the value that an organization provides.[73] The study repeatedly points out that the major problem with the GDPR seems to be a lack of transparency stemming from poor compliance of data holders.[74] Poor compliance typically occurs where data holders respond late, or not at all, to a data breach and hold incomplete data that they fail

[64] EU-US Adequacy Decision, *supra* note 60.
[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] Alex Bowyer et. al., *Human-GDPR Interaction: Practical Experience of Accessing Personal Data*, ASSOCIATION FOR COMPUTING MACHINERY (APR. 2022), https://doi.org/10.1145/3491102.3501947 [https://perma.cc/Q8E5-U2RK].
[69] *Id*. at 3.
[70] *Id*. at 8.
[71] *Id*. at 10.
[72] *Id*. at 12.
[73] *Id*.
[74] *Id*. at 15.

to rectify.[75] This lack of compliance has made consumers feel as though the organizations still hold significant power over their data, which is reinforced by insufficient pressure by regulators.[76]

C. U.S. Response to GDPR—California's Consumer Privacy Act

California followed the E.U. by passing its privacy act, which went into effect on January 1, 2020.[77] The law states that "all people are by nature free and independent and have inalienable rights . . . acquiring, possessing, and protecting property, and pursuing obtaining safety, happiness, and privacy."[78] California is one of five states to have a specific regulation relating to the right to privacy.[79] Some of these provisions closely mirror the Fourth Amendment relating to search and seizure or government surveillance but add specific references to a right to privacy.[80]

The California Privacy Act focuses on:

[A]ny for-profit entity that collects consumers' personal information, or on the behalf of which such information is collected and that alone or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.[81]

Thus, when a consumer requests it, businesses are required to disclose the consumers' rights to their data and the categories of information that could be collected.[82] The goal of the act was to encompass basic internet privacy rights, transfers, and give control back to the consumer. The act also places responsibility on the regulator to enforce the law rather than the consumer.[83]

---

[75] *Id*. at 9.
[76] *Id*.
[77] *California Consumer Privacy Act (CCPA) – an overview*, USERCENTRICS (August 5, 2021) https://usercentrics.com/knowledge-hub/california-consumer-privacy-act/#:~:text=Get%20started!-,What%20is%20the%20CCPA%3F,began%20on%20July%201st%2C%202020 [https://perma.cc/9C3D-RFKR].
[78] CAL. CONST. art. I § 1.
[79] Fredric D. Bellamy, *U.S. Data Privacy Laws to Enter New Era in 2023*, REUTERS (Jan. 12, 2023), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/ [https://perma.cc/CTF6-2L4W].
[80] Pam Greenburg, *Privacy Protections in State Constitutions*, NAT'L CONF. OF STATE LEG. (Jan. 3, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx#:~:text=The%20right%20of%20the%20people,legislature%20shall%20implement%20this%20section.&text=No%20person%20shall%20be%20disturbed,invaded%2C%20without%20authority%20of%20law.&text=All%20people%20are%20by%20nature%20free%20and%20independent%20and%20have%20inalienable%20rights [https://perma.cc/AFR5-BDDV].
[81] Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States*, 23 J. OF TECH. LAW & POL'Y 68, 92 (2018).
[82] *Id*. at 94.
[83] *Id*. at 100.

However, its shortcomings undercut the law's ability to provide the kind of sweeping consumer privacy it hoped to implement.[84] While it hoped to provide protection through stricter consent requirements, the reality is that the California Consumer Privacy Act is just an extension of U.S. consumer privacy laws because it does not prohibit the transfer of personal data to data brokers.[85]

IV. YOU'RE SPENDING WHAT? CREDIT CARDS AND MERCHANT CATEGORY CODES

As technology changes, the conversation around data privacy continues to grow and there have been greater concerns regarding what is being done to keep consumers safe and what is being done to protect corporations. These conversations have significantly increased as credit card histories are being used in controversial areas for the American consumer.

A. Data Mining and Merchant Category Codes

In order to fully understand how the American government and many financial institutions monitor information, it is important to know about data mining, also known as knowledge discovery data, and merchant category codes (MCC).

First, data mining, also referenced as knowledge discovery in data, is the process of uncovering patterns and other valuable information from large data sets.[86] This is used by companies to turn data into useful information.[87] The data can be divided into groups for two different purposes: they can either describe the target dataset or predict outcomes through machine learning algorithms. [88] Ultimately, they help detect fraud and security breaches.[89]

Specifically, within banking systems, credit card purchases are monitored with merchant category codes. MCCs are four-digit numbers that credit card processors assign to businesses for credit card payments.[90] The codes are managed by the International Organization for

---

[84] Salomé Viljoen, *The Promise and Pitfalls of the California Consumer Privacy Act*, DLI AT CORNELL TECH (Feb. 19, 2021), https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act [https://perma.cc/WYB4-GE2V].
[85] *Id*.
[86] *Data Mining*, IBM, https://www.ibm.com/cloud/learn/data-mining [https://perma.cc/H2U8-QR2Q] (last visited Apr. 2, 2024, 2:58 pm).
[87] *Id*.
[88] *Id*.
[89] *Id*.
[90] Dawn Papandrea, *What is a Merchant Category Code (MCC)?,* THE BALANCE (Dec. 29, 2021), https://www.thebalancemoney.com/what-is-a-merchant-category-code-

Standardization (IOS), a group located in Geneva, Switzerland.[91] The IOS maintains the list of codes and assigns them specifically to businesses by bank.[92] The codes classify a merchant into a particular category based on the goods or services it sells most, such as travel, groceries, gas, and so on.[93]

When a consumer pays with a credit card, the MCC is transmitted to the payment processor, such as Visa, Mastercard, or American Express (or whichever creditor the consumer uses).[94] Typically, these codes are used for reward credit systems offered by financial institutions, but are also being used to track consumer spending. Companies will put consumer spending data in a report at the end of the year.[95] So, the MCCs are incorporated to track the kind of purchase being made, without specifically identifying what was bought.[96] For example, if you were to buy food or medicine at a gas station, the MCC would register it as a "gasoline" purchase rather than by the specific items bought. David Shipper, a financial analyst for a research firm, Aite-Novariza Group, stated:

"Merchant codes help define volume and see where things are moving in different types of businesses…without them, it would be really difficult to understand as a card issuer where your consumers are spending money."[97]

For the most part, consumers ignore MCCs and use them simply to gain points to use for travel, food, or other benefits offered by reward cards. However, MCCs are now under attack as being a potential way to monitor dangerous activity by consumers.

B. The Latest Method of Gun Control: Credit Cards

In August 2022, Visa, Mastercard, and American Express announced they would add a new merchant category for firearm retailers.[98] This came as a response to a letter penned by U.S. Senators Elizabeth Warren and Ed Markey, who have been advocating for greater financial involvement in gun control.[99]

5116787#:~:text=card's%20bonus%20rewards.-,What%20Is%20a%20Merchant%20Category%20Code%20(MCC)%3F,or%20services%20it%20sells%20most. [https://perma.cc/G53G-FB37].

[91] Sylvie Douglis, *Can credit card codes help address gun violence?*, NPR (Oct. 17, 2022), https://www.npr.org/transcripts/1129532241 [https://perma.cc/AW2P-SJDZ] [hereinafter "The Indicator"].

[92] *Id*.

[93] Papandrea, *supra* note 90.

[94] The Indicator, *supra* note 91.

[95] Papandrea, *supra* note 90.

[96] *Id*.

[97] *Id*.

[98] Andriotis, *supra* note 2.

[99] *Id*.

Typically, gun shops fall under the MCC category of "specialty retailers or durable goods sellers."[100] However, it is unclear that categorizing firearm retailers with a specific MCC would work because there has been no communication regarding what kind of gun purchases could be deemed suspicious.[101] Andrew Ross Sorkin of the *New York Times* has significantly researched the relationship between financial institutions and mass shooters. Sorkin wrote about the Pulse nightclub shooting when he became curious about how these gunmen were purchasing firearms. Sorkin found that the gunman of the Pulse nightclub shooting had not only charged over $20,000 in weapons on multiple credit cards, but had also researched terms such as "credit card unusual spending" and "why banks stop your purchases."[102]

While this kind of surveillance may bring some peace of mind and could be another step towards stricter gun control policies, this is still an underdeveloped idea. Critics argue that implementing this MCC will not work because it would require stores to work with banks in reclassifying the store.[103] Many have also reemphasized that owning a gun in America is a right constitutionally protected by the Second Amendment.[104] The greatest concern, however, is that the government could use credit cards as a new monitoring device.[105]

The MCC announcement caused people to question the relationship between consumers and financial institutions. Both Visa and Mastercard released statements reiterating their commitment to their customers' privacy.[106] Adding that they do not track personal purchasing habits or block legal transactions based on the MCC.[107] Both credit card companies stated that they do not believe private companies should serve as moral arbiters of consumer purchasing.[108]

Further, in response to these new MCC categories, Republican attorney's generals from twenty-four states warned the credit card companies not to move forward implementing the new codes because they could lead to a misuse of consumer data and would not protect the

[100] The Indicator, *supra* note 91.
[101] *Id*.
[102] *Id.*
[103] *Id*.
[104] Brad Polumbo, *Elizabeth Warren wants your credit card company to report you to the government*, THE WASHINGTON EXAMINER (Sept. 9, 2022) https://www.washingtonexaminer.com/opinion/elizabeth-warren-wants-your-credit-card-company-to-report-you-to-the-government [https://perma.cc/WM77-QD6S].
[105] *Id*.
[106] The Indicator, *supra* note 91.
[107] *Id*.
[108] *Id*.

public.[109] The group, led by Tennessee Attorney General Jonathan Skrmetti and Montana Attorney General Austin Knudsen, stated that they would launch an investigation into the credit card companies: "We will marshal the full scope of our lawful authority to protect our citizens and consumers from unlawful attempts to undermine their constitutional rights."[110]

Moving forward, there seems to be a substantial number of roadblocks that would prevent the effectiveness in preventing dangerous firearm purchases. One big barrier includes determining what would qualify as a suspicious firearm purchase. To start, one requirement would be for all stores that fall under the new MCC firearm code to work with banks to reclassify their stores in alignment with the new codes. There is a significant likelihood that many stores that are selling firearms will not be the first in line to reclassify their stores for this code.

Much like the purchase of firearms, there are other, more personal ways that credit card companies monitor consumer transactions.

V. MONITORING OF CREDIT CARD PURCHASES IN PROSECUTING ABORTIONS

As the government looks to increase its monitoring of credit card payments for gun purchases, the recent overturning of *Roe v. Wade* has led to fear that this could transfer over to abortion purchases. The MCC for health care providers is MCC 8099, which covers "Medical Services and Health Practitioners."[111] While a payment with an MCC would not state what has explicitly been bought, that information can be deduced through the purchase amount or location of the purchase.[112]

As of November 15, 2022, abortion is banned in fifteen states, and it is expected that about half the states in the U.S. will enact bans on abortion or impose other gestational limits on the procedure.[113] Payment trails will likely become a high priority when prosecuting abortions as law enforcement could request patient credit card spending through a subpoena.[114]

Subpoenas are a common means for the government to gather information, and the Fourth Amendment only provides a baseline of

---

[109] AnnaMarie Andriotis, *Visa, Mastercard, Amex Face Calls from GOP Attorneys General to Abandon Gun-Shop Code*, THE WALL ST. J. (Sept. 20, 2022), https://www.wsj.com/articles/visa-mastercard-amex-face-calls-from-gop-attorneys-general-to-abandon-gun-shop-code-11663674954?mod=Searchresults_pos2&page=1 [https://perma.cc/Y7RY-XK54].
[110] *Id*.
[111] *MCC Codes – Merchant Category Codes*, WEB PAYMENT SOFTWARE, https://www.web-payment-software.com/online-merchant-accounts/mcc-codes/ [https://perma.cc/L2QM-LK46] (last visited Mar. 3, 2023).
[112] Lieber & Bernard, *supra* note 1.
[113] *Tracking the States Where Abortion is Banned*, N.Y. TIMES, (Nov. 15, 2022), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [https://perma.cc/7DPT-B6CR].
[114] Lieber & Bernard, *supra* note 1.

protection for consumers.[115] Subpoenas are an order to obtain testimony or documents and must meet a number of criteria to be enforced, but can still be challenged should the recipient allege improper purpose or that the information sought is privileged.[116] Previously, there was a distinction of subpoenas for corporate records (which could be obtained via subpoena) and personal papers (which could not), but the courts have gradually abandoned this distinction.[117] As prosecutions for abortions begin to grow, it is reasonable to assume this type of information requested will become increasingly frequent. Many financial institutions remain silent on how they will respond to these requests.

One bank in particular, Amalgamated Bank in New York, has pledged to scrutinize subpoenas for information sought to prosecute woman and their right to choose.[118] However, other major credit card companies have not made the same commitments. Harvard Law Professor Alejandra Caraballo analyzed many user agreements through various financial institutions and determined that "essentially all [agreements] are bad…they will comply with legal processes and will turn over documents either through warrants or subpoenas."[119] The Vice President of U.S. Policy at Future of Privacy Forum, Amie Stepanovich, stated that often warrants and subpoenas can be accompanied by gag orders that prevent companies from communicating to their customers that they are being investigated.[120]

There should be some restrictions under the Health Insurance Portability and Accountability Act (HIPAA). Yet even under HIPAA, which governs the privacy of a patient's health records, a subpoena allows the release of medical and billing information.[121] HIPAA provides a broad exception for law enforcement, permitting a HIPPA-covered entity to disclose protected health information to law enforcement without notifying the consumer if a subpoena has been issued.[122] With this exception, many are cautiously watching to see how companies and health plans will interpret it with abortion.

While there needs to be a level of cooperation with the court and the subpoenas ordered, the process of getting those orders quashed is burdensome on financial organizations, as there could be any number of investigations occurring at one company. Recently, data-marketing and analytics company Kochava Inc. sued the FTC, raising a claim for

[115] Solove & Schwartz, *supra* note 4, at 275.
[116] Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).
[117] Solove & Schwartz, *supra* note 4, at 276.
[118] Lieber & Bernard, *supra* note 1.
[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] 45 C.F.R § 164.512(f).

marketing geolocation data that might be used to track consumer visits to sensitive locations, such as abortion clinics.[123] Additional measures taken include President Joe Biden issuing an Executive Order that asks the FTC to consider measures to protect the privacy of those seeking online information for reproductive-healthcare services.[124]

VI. MOVING FORWARD: FEDERAL DATA PRIVACY LAW IMPLEMENTED IN THE UNITED STATES

In the discussion of both these hot topic issues, both seem to lead to the same conclusion that it is far too easy for consumer data to be shared among different corporations. It also poses the question of how much margin the government is allowed if its monitoring is presented in the name of safety. Many lawmakers and regulators have discussed the implications of a federal data privacy law, but as fear and division rapidly grow with technological institutions in the U.S., it is time for the U.S. government to start focusing more on the consumer than the corporation. Data has become a traded and exploited commodity for the advantage of corporations, as behavioral insights aid advertisers to serve the corporation ahead of the consumer.[125]

A. The Importance of a Federal Data Privacy Law

The focus on data privacy in the U.S. has been on the consumer's notice and choice. Many have deemed this choice to be a "successful failure," as it portrays the market as one that protects privacy, but ultimately will place blame on the customer's choices for not being proactive enough and seeking out their right to privacy.[126] The conversation should be less about whether this information is used by corporations and marketers and more about the kind of information and notice given to the consumer regarding the kind of information being accessed and potentially used against them.

The monitoring of firearm purchases creates a breach of privacy. While the Fourth Amendment provides some protection, there is a level of government monitoring that seems to overstep. The frustrating part of such government oversteps is that while the right to privacy and data protection are different, many people do not understand how much of their data is being shared. Plus, when increased monitoring is marketed to consumers under the notion that it is for their safety and protection, it almost seems noble. The increased monitoring system of firearms is a

---

[123] John D. McKinnon, *Idaho Company Sues FTC, Claiming Agency Threatened Suit Over Its Tracking Data*, Wall St. J., (Aug. 15, 2022), https://www.wsj.com/articles/idaho-company-sues-ftc-claiming-agency-threatened-suit-over-its-tracking-data-11660608782 [https://perma.cc/F9UR-WFSR].
[124] Press Release, *FACT SHEET: President Biden Issues Executive Order at the First Meeting of the Task Force on Reproductive Healthcare Access*, THE WHITE HOUSE (Aug. 3, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/03/fact-sheet-president-biden-issues-executive-order-at-the-first-meeting-of-the-task-force-on-reproductive-healthcare-access-2/ [https://perma.cc/FW73-ULHV].
[125] Bowyer et. al., *supra* note 68, at 1.
[126] Hoofnagle et. al., *supra* note 43, at 79.

wakeup call, which created more fear with the prosecution of abortions. Even though both issues are incredibly divisive in the U.S., there needs to be a more unified voice in protecting consumers.

While many credit card companies boast about the strength of their fraud protections, many do not mention sharing consumer data. The issues of gun control and abortion are incredibly important and bring to light the notion that even the simple act of sharing basic personal information should be tightly regulated and monitored. One of the major downfalls of the GDPR is the significant lack of transparency when data holders are pressed about what personal consumer information is being shared and used. This has been an issue in the U.S., even despite the substantial focus on notice and consent in privacy laws. The attempt to obtain data from various credit card companies is a tedious process and often takes a significant amount of convincing to get the information a consumer needs. In a country where credit cards account for 57% of transactions, this should not be the case.[127]

While California attempted to create a privacy law that was as expansive and restrictive as the GDPR, the U.S. needs a stricter data privacy law that pulls more from the GDPR rather than expanding on the CCPA. First, is getting entities to think more strategically in the ways they target consumer data, can be accomplished by having corporations comply, which would require creating greater incentives and penalties. Second, as some proposed data privacy plans have attempted in the past,[128] it is important to build upon state regulations instead of imposing a limiting ceiling. Finally, there needs to be a stronger enforcement of transparency between data holders and consumers.

B. Economic Implications

One of the biggest concerns with implementing a strict data privacy regulation similar to that of the GDPR is the economic implications it could cause. The fines imposed by the GDPR could cost companies millions of dollars to meet standards and could severely harm small to medium-sized businesses. If the U.S. adopted provisions mirroring the GDPR, it could cost the U.S. economy $122 billion per year.[129] There is fear that the standard the U.S. should hold major tech companies to for consumer privacy could also be a significant deterrence for smaller

---

[127] Pamela Paul, *The Cost of Going Cashless*, N.Y. TIMES, (Nov. 13, 2022), https://www.nytimes.com/2022/11/13/opinion/cashless-pay-problem.html [https://perma.cc/U5J9-ZDRY].
[128] Hayley Tsukayama, et. al., *Americans Deserve More than the Current American Data Privacy Protection Act*, ELEC. FRONTIER FOUND (Jul. 24, 2022), https://www.eff.org/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act [https://perma.cc/8EGB-Y46V].
[129] Alan McQuinn & Daniel Castro, *The Cost of Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND (August 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/ [https://perma.cc/7HKP-Y45C].

companies. If faced with strict sanctions and fines, matching the six-figure fines in the GDPR, it would be likely that many companies would not take the risk.

The cost mentioned above, expressly mirrors the GDPR, and would be what it would take for companies to comply. Essentially, the U.S. would establish mandates for organizations to appoint data protection officers, boost their budgets to enhance user rights protection, and assess the rise in legal risks. However, the U.S. could focus on the federal data privacy law to reduce costs. For example, focusing on federal and state privacy audits, headed by the FTC, could be a significant way to enforce stricter regulation. While audits cost a significant amount of money (around $444 million[130]), this is in lieu of imposing strict monetary penalties that would create a large burden on corporations. The standard should be set at a federal level and expanded upon by each state, giving them more freedom details and functionality of how audit would be enforced.

The implication of an overly restrictive regulation imposes an incredible amount of cost in the increased standard of compliance. One way to avoid this would be through data minimization. Data minimization is the "collection and retention of the minimum data possible" and is the idea that companies should only collect a minimum amount of necessary information.[131] It also involves the deletion of data that is no longer useful or necessary and setting time limits on this data.[132] This process would require companies to share with consumers how and why they are using their data and not allow companies to use it outside that scope.[133]

A hesitation with data minimization is that it would hurt the U.S. economy by affecting the usefulness of advertisements and how companies generate value from data.[134] However, data minimization could be written in the regulation and state that companies are able to use consumer data for the development of a product and share this information only to enhance that experience, but not share this information with advertisers. While advertising is an important facet of the U.S. economy, advertisers do not need a lot of specific personal information to do their job. Implementing a broader form of data minimization could help the consumer understand what kind of personal information is used by corporations and narrow the scope of how much information is being collected.

While an overly strict regulation may create a cost burden on companies, this could be remedied by placing a greater responsibility on

---

[130] *Id*.
[131] Md. Abdul Malek, *Bigger is Always Not Better; less is More, Sometimes: The Concept of Data Minimization in the Context of Big Data*, 2021 EUR. J. PRIVACY L. TECH. 212, 215 (2021).
[132] *Id*. at 216.
[133] McQuinn & Castro, *supra* note 129.
[134] *Id*.

federal and state regulators to hold corporations accountable. However, some might argue that invoking a private right of action creates more legal fees and increase of cost, but it creates a greater incentive for companies to comply with the federal standard. Also, many companies often have arbitration agreements in their user agreements, which would help persuade companies to comply without the threat of litigation which lowers the cost of legal fees.[135] However, in advocating for consumer rights, consumers should still have the right to raise concerns over harms caused by corporations. This would also take a huge burden off the FTC as they are now monitoring a vast amount of privacy policies and violations and allow for harm to be dealt with quickly and more efficiently.

While the standard of data minimization and others can be nuanced, it points to the need for a federal law that sets a broad standard and encourages each state to expand and narrow in their own ways.

C. State Partnership

When implementing federal data privacy regulation, the law should work alongside state laws rather than creating an overbearing ceiling. This concept, known as preemption, allows the federal government to prevent state and local governments from passing competing or contradictory privacy laws that may confuse consumers and increase compliance costs.[136] As many states are now implementing provisions protecting consumer privacy in state constitutions, there is fear that a federal privacy law that is too strict and narrow could limit and harm protections offered by states. As Congress considers the regulations to impose regarding privacy, it should first look to what states are already implementing and use that information to build and enhance the federal law. Providing a good baseline for the federal law, states can still provide protections in ways they see fit while operating within a structured federal framework.

By leveraging the diverse experiences and perspectives of individual states, federal policymakers can gain invaluable insights into the intricacies of safeguarding consumer privacy. This collaborative approach not only ensures that federal standards are informed by real-world challenges but also fosters a sense of ownership and accountability among state governments. Moreover, by embracing state-level innovations and best practices, federal regulations have the potential to create a synergistic framework that offers robust and adaptable protections for consumers nationwide.

---

[135] Tsukayama, et. al., *supra* note 128.
[136] McQuinn & Castro, *supra* note 129.

This is also important in relation to gun control and abortion laws. These two issues are already divisive, but every state is passing different laws for both issues. The beauty of this country is that each state has the freedom to establish their own specific regulations. However, due to the divisive nature of all three issues of gun control, abortion, and privacy, the standard set by the federal government is extremely important. It sets the tone of what will be the broad foundation for the states to build upon in their own legislation.

D. Transparency in Consumer-Corporation Relationship

Finally, many criticize privacy regulations, stating there is a lack of transparency between data holders and consumers. The GDPR received criticism when a study revealed that the regulation had minimal impact on the transparency of communication with companies and consumers. In the U.S., there have been a few journalists that have investigated credit card companies and how they use data, but often left the investigations frustrated and without a solid answer.[137] The requirement within a federal regulation regarding consumer information and how it is used ought to be accessible and easy to retrieve.

The tech industry is massive, and companies have a considerable amount of information on each consumer that uses its services, but when asked, consumers should not have to turn into an investigative journalist to receive the information. It should be required that, upon request, the information provided back to the consumer should be in plain language. A consumer should not be expected to have a vast technical background and knowledge needed to interpret consumer data. Providing notice to the consumer is important but loses its significance if the consumer requests more information only to find they need to thoroughly investigate every technology company that may have access to their data.

Credit card companies will communicate with their customers when their financial information is requested, but what about when this information is being tracked? As mentioned above, the increased monitoring of MCCs is a cause of concern for many because, while it may be marketed to the consumer that this monitoring is for safety purposes, it seems as though it is more an encouragement for credit cards to be used less and for troubling behavior to be implemented in an even more vague manner. This would also apply to abortions. If the government and credit card companies continue to partner with each other to monitor citizen's financial transactions, it would likely push the consumer to use physical money and discover methods to keep these purchases as discreet as can be. While it could be argued that these financial statements are already being monitored for white collar crimes and money laundering, it seems as though this kind of monitoring has

[137] Kashmir Hill, *Amazon and Chase Will Not Give Me a Straight Answer About What They do with My Credit Card Data*, GIZMODO (Jan. 23, 2019), https://gizmodo.com/neither-amazon-nor-chase-will-give-me-a-straight-answer-1831882327 [https://perma.cc/9VZ2-Y8DZ].

already caused concern for going beyond the scope of what has been communicated.[138] Ultimately, Americans are deliberating the permissible extent of governmental surveillance over their financial records in the pursuit of safety.

VII. CONCLUSION

As the U.S. becomes increasingly divided regarding issues of abortion and gun control, data privacy emerges as a unifying concern for many. The need for a federal law enforcing government monitoring has become evident, aiming to provide greater incentives and penalties for corporate compliance. This law encourages entities to strategize how they target consumer data, building upon existing state regulations rather than imposing limiting restrictions. Moreover, it advocates for stronger enforcement of transparency in the relationship between data holders and consumers.

As technology grows and develops, lawmakers should advance with these rapid developments to best protect their consumers in the face of a significant invasion of privacy. It is paramount that consumer interests take precedence over corporate interests. Therefore, the United States should prioritize the implementation of a federal data privacy law to promptly address these pressing privacy concerns.

[138] Andriotis, *supra* note 2.