DESPERATION FOR LEGISLATION: THE NEED FOR THE AMERICAN DATA PRIVACY AND PROTECTION ACT

ANDREW P. QUAY*

ABSTRACT

Protecting personal data is becoming increasingly relevant as technology continues to advance. But many countries fail to meet the urgency of building the necessary legal protection. This Comment analyzes why current data privacy law in the United States is insufficient to shield the data of more than three hundred million citizens. Without comprehensive data privacy law, the sensitive data of Americans are at frequent security risk. Combating this risk is imperative. To do so, as this Comment will explain, the United States needs to learn from European, namely Swiss, advancement and pass comprehensive legislation. The American Data Privacy and Protection Act represents its best chance.

* Andrew P. Quay is a 2024 J.D. candidate at the University of Wisconsin Law School. Following graduation, Andrew will be practicing real estate and employment litigation in Minneapolis, MN. Andrew extends his sincerest gratitude to the hard-working staff of the *Wisconsin International Law Journal* for their time during the writing and publication process. He is especially thankful for his mother, Kathryn, for her unwavering support throughout his academic journey.

https://doi.org/10.59015/wilj.RRZV1592

INTRODUCTION

Data privacy is under attack. In April of 2011, Sony was hit with a groundbreaking cyberattack, compromising the names, addresses, and potentially even credit card information of tens of millions of people.[1] In May of 2017, malware files struck computer systems across the world, compromising the personal data of citizens from more than seventy countries.[2] With the growth of the internet and its increased accessibility, more and more users are at risk of falling victim to privacy intrusions.[3]

Some countries, like Switzerland, have spearheaded efforts to defend data privacy and have effectively combated privacy threats. Others, like the United States, remain short of the mark in this ever-changing climate of technology and its many threats to data privacy. This Comment will analyze and criticize the United States' disfigured approach to addressing data privacy law. It will illustrate why, instead of delegating data privacy by sector and state, Congress should pass the American Data Privacy and Protection Act (ADPPA) to model Switzerland's federal oversight for the benefit of consumers in a privacy-threatening world.[4]

Many countries and international organizations have stepped up to the plate to combat ever-increasing privacy threats.[5] Most notably, the European Union set the gold standard in May of 2018 by enacting the General Data Protection Regulation (GDPR).[6] The GDPR established a broad protection in pursuit of persons having a "fundamental right" to "the protection of personal data."[7] Prioritizing the privacy of European Union citizens over profits, the GDPR threw the privacy policies of notable

---

1 McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 644–45 (2012).

2 Marcelo Triana, *Is Selling Malware a Federal Crime?*, 93 N.Y.U. L. REV. 1311, 1312 (2018).

3 Cunningham, *supra* note 1, at 645.

4 American Data and Privacy Protection Act, H.R. 8152, 117th Cong. (2022).

5 Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734 (2021).

6 Council Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) 1.

7 *Id.*

companies like Amazon, eBay, and Facebook out of compliance.[8] Legislative response to the GDPR, or lack thereof, has drastically varied between countries.

Unfortunately, the United States has not followed suit in adopting similar, widespread data privacy law. In failing to do so, the United States exposes its citizens to data privacy threats. While there have been a handful of Congressional attempts at overarching data privacy legislation, each has failed to become law.[9] Switzerland, on the other hand, has taken quick action to follow the GDPR. Going beyond mere attempts, the Swiss Parliament has put data privacy at the forefront of our constantly evolving technological environment.

This Comment will explore the increasing importance of data privacy law with the onset of globalization and the internet. It will examine the histories of Swiss and United States data privacy law to explain the formation of their stark structural differences. It will also spotlight the American Data Privacy and Protection Act, a recently introduced bill in the House.[10] To provide context, this Comment will explore the weaknesses of current data privacy laws in the US, comparing them with the simplistic but strong Swiss laws. Finally, in light of these comparisons, this Comment will argue why passing the American Data Privacy and Protection Act is crucial to better protect consumers' data privacy.

I. BACKGROUND

Despite the looming data privacy threats, many countries fail to enact overarching legislation. Data privacy laws in the United States—split between states and sectors—are disfigured and leave endless room for privacy threats. A few states' attempts to model the GDPR are insufficient to protect the entire American citizenry. On the other end of the spectrum, the Swiss Parliament stays clear of the United States' inconsistencies by revamping its data privacy laws. In doing so, combined with its constitutional protection, Swiss data privacy remains a guiding light for countries like the United States.

---

[8] Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 391–93 (2019).

[9] *See, e.g.*, Data Accountability and Trust Act, H.R. 1282, 116th Cong. (2019) (requiring stricter security practices, notice obligations, and civil penalties); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (requiring privacy transparency, designated privacy officials, and prohibiting harmful data practices).

[10] American Data and Privacy Protection Act, H.R. 8152, 117th Cong. (2022).

A. SWISS DATA PRIVACY LAW

A model for other nations, the Swiss data privacy framework is composed of two major laws: the Federal Constitution of Switzerland and the new Federal Act on Data Protection (nFADP).[11] Swiss companies also comply with the GDPR when conducting business in the European Union, but this Comment will not discuss GDPR requirements.

Unlike that of the United States, Switzerland's constitution contains data privacy regulations.[12] Among fundamental rights such as the freedom of expression and freedom of assembly, Article 13 of the Federal Constitution of Switzerland includes a right to privacy.[13] But the protection of Swiss data does not end at the border.

Swiss data privacy is also protected outside of the country by the nFADP.[14] Established in 1992, the original FADP came into effect prior to the rapid expansion of the internet and has gone through many necessary revisions.[15] It had one purpose—to protect the data of natural (humans) and legal (associations) parties processed by private persons and federal bodies.[16] To do so, the FADP shifted power from data controllers (private persons and federal bodies) to consumers in two respects. First, it allowed consumers to request information about whether their data was being processed.[17] Second, it required voluntary consent by the consumer for the processing of their data.[18] In doing so, the FADP established Swiss data privacy law beyond its own borders until the expansion of the internet begged for updated protection.

Considering the FADP outdated, the Swiss Parliament passed the nFADP in 2020 to take its place.[19] The nFADP was implemented in

---

[11] BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101; BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] Sept. 25, 2020, SR 235.1, AS 491.

[12] *See* BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101, art. 13.

[13] *Id.*

[14] BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] Sept. 25, 2020, SR 235.1, AS 491, art. 3.

[15] FED. DATA PROT. AND INFO. COMM'R, THE NEW DATA PROTECTION ACT FROM THE FDPIC'S PERSPECTIVE 2 (2021).

[16] BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] June 19, 1992, SR 235.1 (1993), arts. 1, 2 *as amended by* Gesetz, Sept. 25, 2020, AS 491 (2022).

[17] *Id.* art. 8.

[18] *Id.* art. 4.

[19] FED. DATA PROT. AND INFO. COMM'R, *supra* note 15, at 3.

September of 2023, and it required companies to comply by that date.[20] Modeled after the gold standard GDPR, the nFADP marks a shift from protection of both legal and natural persons to just natural persons.[21] But this does not warrant worry thanks to newfound requirements.

The nFADP significantly tightens the privacy requirements of its predecessor. It increases criminal penalties and introduces privacy certification measures, for example.[22] Thankfully, companies already in compliance with the GDPR will have minimal changes to make to their privacy practices.[23] This avoids a potential loss of competitiveness for Swiss companies by allowing the free flow of data between Switzerland and the European Union.[24]

In sum, Swiss data privacy law remains strong through continuous adaptive revisions. Learning from the GDPR, the Swiss Parliament completely revamped the FADP to meet privacy demands with the growth of the internet. With Article 13 putting constitutional protection of data privacy in place, Swiss data privacy law is only further bolstered by legislative action. Many other countries, such as the United States, have failed to meet such a degree of attention to data privacy law.

B. GAPS IN US DATA PRIVACY LAWS

Data privacy laws across the United States are split between states and business sectors.[25] Without an umbrella of federal oversight, and with the onset of the GDPR, US consumers have been struck with a series of privacy policy emails.[26] Awaiting a federal response, several states took matters into their own hands by enacting legislation to comply and protect citizens' data privacy.[27]

Just one month after the GDPR went into effect, California passed the California Consumer Privacy Act in response.[28] Much like the GDPR,

---

[20] *New Federal Act on Data Protection (nFADP)*, SME PORTAL, https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html [https://perma.cc/TR8Q-2ZJA].

[21] FED. DATA PROT. AND INFO. COMM'R, *supra* note 15, at 3.

[22] *The Main Provisions*, FED. DATA PROT. & INFO. COMM'R, https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/ndsg.html [https://perma.cc/3P8Y-9FW7].

[23] *New Federal Act on Data Protection (nFADP)*, *supra* note 20.

[24] *Id.*

[25] Chander et al., *supra* note 5, at 1738.

[26] *Id.* at 1734.

[27] *Id.*

[28] CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2023).

the California Consumer Privacy Act empowers consumers with the rights to know how their data is used, to delete collected data, to opt out of the sale of their data, and to enjoy nondiscrimination for exercising these newfound rights.[29] California is one of several states that have chosen not to wait for a federal response. Colorado, Utah, and Virginia have passed similar legislation,[30] the important differences of which will be explored later.

Separate from state action, Congress has been successful in passing sector-specific data privacy laws.[31] The Health Insurance Portability and Accountability Act, better known as HIPAA, protects health information from being shared without consent.[32] The Family Educational Rights and Privacy Act, or FERPA, protects data in student educational records.[33] Specifically, it gives minors and parents the option to not disclose information that could damage a student's future.[34] Lastly, the Children's Online Privacy Protection Act (COPPA) protects children under the age of thirteen by imposing strict regulations on how their data is handled.[35] In doing so, the goal is to protect children from online predation.[36]

These three sectoral examples show that Congress has implicitly chosen to value certain personal information related to health, education, and children. While any protection is valuable, data privacy laws between states and the private sector give way to dire security risks.[37] Trying to bridge these gaps, many members of Congress have proposed bills that, if enacted, would provide federal protection to data privacy.[38]

---

[29] *See generally id.*

[30] COLO. REV. STAT. §§ 6-1-1301 to -1313 (2021); UTAH CODE ANN. § 13-61-101 to -404 (West 2023); VA. CODE ANN. §§ 59.1-593 to -602 (2023).

[31] Rebecca Lipman, *Online Privacy and the Invisible Marker for Our Data*, 120 DICK. L. REV. 777, 787 (2016).

[32] *See generally* Health Insurance Portability and Accountability Act, H.R. 3103, 104th Cong. (1996).

[33] 20 U.S.C. § 1232g.

[34] *See id.* § 1232g(b).

[35] *See* 15 U.S.C. § 6502.

[36] *See id.*

[37] *See* Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?*, 27 CATH. U. J.L. & TECH. 77, 83–84 (2018); Michael P. Goodyear, *A Rising Tide Lifts All Consumers: Penumbras of Foreign Data Protection Laws in the United States*, 27 RICH. J.L. & TECH. 1, 2 (2020).

[38] *See infra* note 41.

1. Congressional Attempts at Data Privacy Law

Despite staggered attempts, the US Congress has remained unable to pass a bill that federally encompasses data privacy beyond individual states and sectors.[39] Reaching for a more stable federal oversight, these attempts from both the House and Senate have shared the common goal of uniform protection.[40]

Few of Congress's attempts at broad data privacy bills have passed.[41] Unfortunately for American citizens, this implies a bipartisan lack of initiative. A more recent bill to pass in the House, encompassing data privacy, is the Data Accountability and Trust Act.[42] However, even this bill, with the simple purpose of providing "reasonable security policies and procedures" was too much to pass on both sides of the aisle.[43] Mustering enough support in the House or Senate, and then breaching the partisan threshold on the other side, has proven impossible for many bills. But recently introduced legislation brings newfound hope to overcome these obstacles.

2. The American Data Privacy and Protection Act

The American Data Privacy and Protection Act (ADPPA) represents a culmination of Congress's staggered attempts at uniform data privacy legislation. Introduced in the House on June 21, 2022, the ADPPA proposes fundamental data privacy regulation.[44] Its purposes are to (1) provide consumers with "foundational data privacy rights," (2) create "strong oversight mechanisms," and (3) "establish meaningful enforcement."[45] Covered entities under the ADPPA generally include, absent an exception,

---

[39] *See* Ariel E. Wade, *A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty*, 42 GEO. WASH. INT'L L. REV. 659, 662 (2010).

[40] *See, e.g.*, Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009); Mind Your Own Business Act, S. 1444, 117th Cong. (2021).

[41] *See, e.g.*, Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (requiring transparency, designated privacy officials, and prohibiting harmful data practices); Mind Your Own Business Act, S. 1444, 117th Cong. (2021) (requiring periodic reporting, assessments, and opt-out processes); Own Your Own Data Act, S. 806, 116th Cong. (2019) (providing privacy autonomy for individuals across social media companies); Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. (2021) (requiring affirmative consent, understandable policies, opt-out options, and bi-annual privacy audits).

[42] Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009).

[43] *Id.*

[44] *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[45] *Id.* pmbl.

any entity or person that alone or jointly determines the purpose and method of collecting, processing, or transferring data.[46] Striving to meet its purposes, the ADPPA is composed of three principle compliance requirements for covered entities: a duty of loyalty, respect for consumer data rights, and corporate accountability.[47]

The duty of loyalty imposed by the ADPPA would keep companies from collecting too much data.[48] Considering the many gaps in current data privacy laws across the United States, this may sound too good to be true. While pessimism is understandable, it is misplaced, as the duty of loyalty in fact keeps businesses from collecting, processing, or transferring data beyond what is "reasonably necessary and proportionate" to the product, service, or communication it provides.[49] Keeping businesses to this standard, the ADPPA allows for the collection, process, or transfer of data, so long as a business demonstrates meeting this standard of reasonably necessary and proportionate.[50]

The consumer data rights endowed by the ADPPA are meant to bolster consumer awareness and business transparency.[51] To that end, consumers must be given rights to access, correct, and even delete their personal data.[52] This access includes giving consumers the autonomy to expressly consent for the transfer of their data and to reserve the right to withdraw that consent.[53] In terms of business transparency, the ADPPA requires that covered entities make their privacy policies comprehensible.[54] In this regard, acceptable privacy policies under the ADPPA must be publicly available in a "clear, conspicuous, not misleading, and readily available manner."[55]

Corporate accountability demanded by the ADPPA means keeping a watchful eye on large data holders. One year after its enactment, large data holders are required to annually certify that they maintain (1) internal controls reasonably designed to comply with the ADPPA and (2) reporting structures to ensure that officers are involved in and are responsible for

---

[46] *Id.* § 2(9)(A)(i).
[47] *See id.* §§ 101, 201, 301.
[48] *Id.* § 101.
[49] *Id.* § 101(a)(1)–(2).
[50] *Id.* § 101(b).
[51] *Id.* §§ 201, 202.
[52] *Id.* § 203.
[53] *Id.* § 204.
[54] *See id.* § 202(a).
[55] *Id.*

maintaining such compliance.[56] Each data holder must designate at least two officers, one privacy officer and one data privacy officer.[57] Beyond ensuring compliance, these designated officers shall, at a minimum, implement data privacy and security programs to protect covered data.[58]

The ADPPA enforces compliance by giving the state and individuals routes to recovery.[59] The state may bring civil action to curb violations of the ADPPA through attorneys general.[60] Likewise, individuals may sue entities making such violations starting four years after the ADPPA's enactment.[61] While both the state and individuals can sue, their potential recoveries will differ. The state may recover injunctive relief, enforce compliance, damages or other appropriate civil penalties, and collect reasonable attorneys' fees.[62] Individuals, on the other hand, may recover sustained damages, injunctive relief, and reasonable attorneys' fees.[63] These lists of recovery options embody and highlight the ADPPA's goal of general data protection.[64] Covered entities will both be deterred from interfering with the ADPPA and forced to comply through injunctions.

The ADPPA makes enforced compliance a last resort. To avoid enforcement, the ADPPA creates the Bureau of Privacy, the purpose of which is to assist the Federal Trade Commission in ensuring consumer protection.[65] Upon enactment, the director of the Bureau of Privacy shall create an Office of Business Mentorship to assist covered entities in their compliance efforts.[66] Covered entities may request advice from the Office of Business Mentorship with regard to actions that could conflict with the ADPPA.[67] Hence, the ADPPA serves as a protective measure first, as opposed to a forced compliance threat.

---

[56] *Id.* § 301(a)(1)–(2).
[57] *Id.* § 301(c)(1)(A)–(B).
[58] *Id.* § 301(c)(2)(A)–(B).
[59] *See id.* §§ 402, 403.
[60] *Id.* § 402.
[61] *Id.* § 403(a)(1).
[62] *Id.* § 402(a)(1)–(4).
[63] *Id.* § 403(a)(2)(A)–(C).
[64] *Id.* pmbl.
[65] *Id.* § 401(a)(1).
[66] *Id.* § 401(b).
[67] *Id.*

II. ANALYSIS

The United States and Switzerland stand on opposite ends of the data privacy law spectrum. Their respective scopes resemble the differences between a microscope and telescope. United States data privacy law, much like a microscope, zooms in on specific individuals and areas without addressing the country as a whole. In contrast, Swiss data privacy law, like a telescope, captures a larger picture encompassing a vast array of individuals and geographic areas. In light of Swiss federal oversight and growing European adoption of broad coverage, the United States needs to pass the ADPPA to meet the demands of a rapidly globalizing world. Its state-and-sector approach to data privacy protection has proved insufficient.

A. ADDRESSING GAPS IN US DATA PRIVACY LAW

Using the GDPR as a model, California, Virginia, Colorado, and Utah have enacted data privacy legislation to meet the growing needs of their citizens.[68] Much like the GDPR, the California Consumer Privacy Act is recognized as the strongest state data privacy law.[69] It provides consumers with the rights to know how their data is used, to delete collected data, to opt out of the sale of their data, and to enjoy nondiscrimination for exercising their newfound rights.[70] In doing so, it protects consumers by applying to businesses that (1) have annual gross revenues exceeding $25 million, (2) receive or share the data of fifty thousand or more consumers, households, or devices, or (3) derive 50 percent or more of their revenue from selling data.[71]

Virginia's Consumer Data Protection Act shares many similarities with the California Consumer Privacy Act. Covered businesses under either California's or Virginia's jurisdiction bear the same responsibilities.[72] The key difference between the two laws is their respective scopes. Virginia's law only applies to businesses that control or process personal data "of at least 100,000 consumers" or "of at least 25,000 consumers and

---

[68] Frederic 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/47CL-6FZK].

[69] Daniel Solove, *A Federal Comprehensive Privacy Law*, YOUTUBE (Aug. 10, 2022), https://www.youtube.com/watch?v=XuSV4c5BSs4.

[70] CAL. CIV. CODE §§ 1798.105, 1798.110, 1798.120, 1798.125 (West 2023).

[71] *Id.* § 1798.140(d)(1)(B).

[72] VA. CODE ANN. §§ 59.1-593 to -602 (2023).

derive over 50 percent of gross revenue from the sale of personal data."[73] While both California and Virginia provide broad state protection over consumer data, covered businesses under each law will vary.

Joining California and Virginia, Colorado and Utah have also taken significant strides in data privacy legislation.[74] The Colorado Privacy Act establishes data privacy as a fundamental right by equipping consumers with, among other rights, the rights to opt out of sharing, to access, to correct, and to delete their data.[75] It applies to businesses that either control or process data "of at least 100,000 consumers" or "derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers."[76] Following the trends of other state data privacy laws, Utah's Consumer Privacy Act provides consumers the rights to access and delete certain personal data as well as opt out of the collection and use of their data.[77] Pulling from the scopes of different states, Utah's Consumer Privacy Act applies to businesses that (1) conduct business in the state or target Utah residents, (2) have an annual revenue of $25 million or more, and (3a) control or process data of one hundred thousand or more consumers, or (3b) derive over 50 percent of their gross revenue from the sale of data and control the data of twenty-five thousand or more consumers.[78]

No two state data privacy laws are the same. While Utah and California have the same annual and gross revenue requirements, they have different consumer data processing limit qualifications to apply. Unlike California, Virginia, or Utah, the Colorado Privacy Act does not have a percentage of gross revenue requirement.[79] Given these many differences, the same company conducting business in two or more states may have to comply with one state's laws but not another's. This staggered structure creates headaches for companies and legislatures alike.

On top of these differences, the actions of these few states cannot adequately protect the entire American citizenry. State laws only apply within respective state boundaries. Whether additional states will join in enacting data privacy legislation remains a guessing game. Even if every

---

[73] *Id.* § 59.1-576.

[74] COLO. REV. STAT. §§ 6-1-1301 to -1313 (2023); UTAH CODE ANN. §§ 13-61-101 to -404 (West 2023.

[75] COLO. REV. STAT. § 6-1-1306(1)(a)–(d) (2023).

[76] *Id.* § 6-1-1304(b)(I)–(II).

[77] UTAH CODE ANN. § 13-61-201 (West 2023).

[78] *Id.* § 13-61-102(1)(a)(i)–(c)(ii).

[79] *See generally* COLO. REV. STAT. §§ 6-1-1301 to -1313 (2023).

state legislature were to suddenly pass such legislation, their provisions would inevitably vary, posing a weak solution.[80] Hence, businesses would have the incredible burden of complying with different state requirements.

1. US Data Privacy Laws without the ADPPA

Differences between state data privacy laws beg for federal uniformity. Separate from state action, Congress has been successful in passing sector-specific data privacy laws.[81] HIPAA, FERPA, and COPPA are worthy of the spotlight here because of their heavy lifting in the realm of data privacy.

HIPAA protects private health information from being shared without consent.[82] It applies to health insurers and medical providers, including their subcontractors.[83] Hence, its protection is limited in two respects: by the type of data at issue, and by the groups collecting that data.

FERPA shields important data in student educational records.[84] Specifically, it gives minors and parents the option to not disclose information that could damage a student's future.[85] However, it only applies to federally funded schools, leaving many students' data out of the picture.[86]

Lastly, COPPA protects children under the age of thirteen by imposing strict regulations on how their data is handled.[87] It only applies to operators of online services—such as websites—that are directed at children or that collect data from children under the age of thirteen to the operator's actual knowledge.[88] While the goal is to protect children from predation, COPPA fails to safeguard minors over the age of thirteen.[89]

The provisions of sectoral data privacy laws inherently vary due to the type of data they protect. As shown, these laws cover narrowly defined data that sector-specific entities handle, from personal health information to student records and data concerning young children.[90] The

---

80 *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1835, 1848 (2010).

81 Lipman, *supra* note 31, at 787.

82 *See generally* Health Insurance Portability & Accountability Act, H.R. 3103, 104th Cong. (1996).

83 *Id.*

84 20 U.S.C. § 1232g.

85 *Id.* § 1232g(b).

86 *Id.* § 1232g(a)(1)(B).

87 15 U.S.C. § 6502.

88 *Id.* § 6502(a)(1).

89 15 U.S.C. §6501(1).

90 William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 977 (2016).

striking downfall of sectoral data privacy laws, like state laws, is their limited scope. These laws are far from comprehensive, as they do not cover most private data handling in the United States.[91]

Left with narrow data privacy protection from state and sectoral laws, courts have resorted to interpreting constitutional amendments in an attempt to fill the gaps.[92] The fact that the United States Constitution is one of the oldest written constitutions still in use today complicates this modern predicament.[93] Since the Constitution is practically unamendable, courts have good reason to instead interpret preexisting amendments to address data privacy gaps.[94] The Supreme Court has held that interpretations of constitutional privacy protections limit government and public interference.[95] In doing so, the Supreme Court has approached data privacy by attempting to unveil implicit protections within the Constitution as opposed to creating an explicit constitutional right to data privacy.[96] The First and Fourth Amendments have generated significant privacy protections through case law.[97]

The Supreme Court has interpreted the First Amendment to contain data privacy rights—indeed, such rights are necessary to exercise the fundamental freedoms of speech and expression.[98] Looking to the freedom of speech, the Supreme Court in *McIntyre v. Ohio Elections Commission* found it necessary to honor an anonymous author's wish to remain anonymous.[99] This is because the interest in including anonymous works in the marketplace of ideas "unquestionably outweighs" public interest in demanding disclosure.[100] In other words, encouraging an individual's freedom of speech trumps the majority's wish for transparency.[101]

The Supreme Court has interpreted the Fourth Amendment to prohibit unreasonable law enforcement searches as well as unreasonable

---

91 *Id.*

92 *Id.* at 975–76.

93 *See* Elai Katz, *On Amending Constitutions: The Legality and Legitimacy of Constitutional Entrenchment*, 29 COLUM. J.L. & SOC. PROBS. 251, 251 (1996).

94 *Id.*

95 DeShaney v. Winnebago Cnty. Dep't. of Soc. Servs., 489 U.S. 189 (1989) (holding that constitutional rights do not restrain the actions of private actors).

96 *See, e.g.*, NASA v. Nelson, 562 U.S. 134 (2010); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977); Whalen v. Roe, 429 U.S. 589 (1977).

97 McGeveran, *supra* note 90, at 976.

98 *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Stanley v. Georgia, 394 U.S. 557 (1969); U.S. CONST. amend. I.

99 514 U.S. at 341–42.

100 *Id.* at 342.

101 *Id.* at 356–57.

searches in public schools and government workplaces.[102] For example, in *Riley v. California*, the court questioned whether police officers could search the digital data of an arrestee's cellphone without a warrant.[103] The inherent conflict in this analysis is what meets the standard of reasonableness.[104] In this regard, a warrantless search is reasonable if it falls within an exception to the Fourth Amendment's warrant requirement.[105] Whether a fact pattern fits within one of these exceptions is up to the court's discretion. By relying on this ambiguous case-by-case analysis, at least in the criminal context, citizens' data privacy rights are subject to the perspective of courts as opposed to stable, written federal protection. This can lead to inequitable results based on what the bench considers reasonable.

The unstable interpretations of constitutional amendments are ill-suited to protect the American citizenry's data privacy. An implied right will always come second to an express one.[106] Individuals could try falling back on the select few cases where the Supreme Court has found data privacy protection in reading between the lines of the Constitution. However, this would not be a feasible strategy. These interpretations could always be overturned, whereas written amendments are likely here to stay.[107]

The United States is not equipped to handle data privacy without comprehensive federal law.[108] Recalling the United States default rule that data collection and processing are fair game unless legislation says otherwise, the gaps left between state laws, sectoral laws, and interpretations of constitutional amendments give way to massive gaps in data privacy protection.[109] As shown, the varied scopes of these provisions are staggered and only apply to certain sets of individuals and actions. Enacting legislation is the most feasible way to address this disfigurement.

---

[102] U.S. CONST. amend. IV; Riley v. California, 573 U.S. 373 (2014) (law enforcement searches); Katz v. United States, 389 U.S. 347 (1967) (law enforcement searches); New Jersey v. T.L.O., 469 U.S. 325, 325 (1989) (public schools); O'Connor v. Ortega, 480 U.S. 709, 709 (1987) (government workplaces).

[103] 573 U.S. at 373.

[104] *Id.* at 378.

[105] *Id.*

[106] *See* McGeveran, *supra* note 90, at 975–76.

[107] *See id.* at 975.

[108] Michael P. Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law*, 10 HOUS. L. REV. 76, 86 (2020).

[109] *See* McGeveran, *supra* note 90, 973–76.

2. How the ADPPA Fills the Gaps in US Data Privacy Laws

Passing the ADPPA is critical for three reasons.[110] First, and most importantly, it would fill the gaps left in state and sectoral laws by providing broad coverage.[111] Second, addressing data privacy is critical in a rapidly globalizing world.[112] Finally, the ADPPA would help the United States catch up to the growing European trend of comprehensive data privacy law.[113]

Passing the ADPPA is necessary to fill the apparent gaps in US data privacy laws. State laws, sectoral laws, and interpretations of a few constitutional amendments have been shown to be insufficient to protect the American public at large.[114] The ADPPA circumvents these insufficiencies by pulling from existing state laws and the GDPR to start the conversation on comprehensive data privacy.[115] It draws from the respective data privacy laws of California, Colorado, Connecticut, Utah, and Virginia, but it adds in notions found in the GDPR, such as corporate accountability and civil rights.[116]

Filling the gaps in data privacy laws across the United States is critical to meeting the inherent privacy risks of a rapidly globalizing world. These gaps give way between the collection, use, and dissemination of data.[117] The ADPPA's data minimization rules, robust individual rights, protections against discrimination, and private causes of action directly address these risks.[118] By opening the doors to private litigation, the ADPPA can be a first step to stopping harmful business practices and holding businesses accountable for noncompliance.[119]

Passing the ADPPA would catch the United States up to the European trend of comprehensive data privacy law. At the core of the GDPR, scaring many US businesses into compliance, is corporate

---

[110] Solove, *supra* note 69.

[111] McGeveran, *supra* note 90, at 975.

[112] Ryan Moshell, *... And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 359–60 (2005).

[113] *Id.*

[114] *See* McGeveran, *supra* note 90, at 974, 976–77.

[115] Solove, *supra* note 69.

[116] David Stauss, *Analyzing the American Data Privacy and Protection Act*, YOUTUBE (Sept. 2, 2022), https://www.youtube.com/watch?v=CMCpfaEZalU [https://perma.cc/JZ5E-MCDP].

[117] Wayne Unger, *Katz and COVID-19: How a Pandemic Changed the Reasonable Expectation of Privacy*, 12 HASTINGS SCI. & TECH. L.J. 39, 42, 60 (2020).

[118] Solove, *supra* note 69.

[119] *Id.*

accountability.[120] The GDPR holds corporations accountable with the potential for significant fines.[121] In pursuit of corporate accountability, Article 5 of the GDPR outlines transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality provisions.[122] The ADPPA strives to meet many of these provisions by limiting the data covered entities may collect, process, and transfer to what is "reasonably necessary and proportionate."[123] This limitation requires transparency, purpose, minimization, accuracy, and integrity by narrowing the scope of allowable data while also covering entities on a federal level.

The ADPPA is just the beginning of comprehensive US data privacy law. While it is not the end-all-be-all, it is certainly a step in the right direction. Since passing the House Committee on Commerce and Energy, the ADPPA has surpassed all its predecessors in the realm of comprehensive data privacy bills.[124] Certainly, this is a positive sign for the progression of data privacy law. That being said, the ADPPA does not account for certain data types such as deidentified data, employee data, and publicly available data.[125] Nonetheless, the ADPPA gets the conversation about comprehensive data privacy law started. This puts the United States on more equal footing with much of Europe, such as Switzerland.[126]

B. THE FEDERAL UNIFORMITY OF SWISS DATA PRIVACY LAW

The Swiss Constitution and Federal Act on Data Protection have been the foundation of Swiss data privacy law.[127] Together, since the implementation of the new Federal Act on Data Protection, there are few gaps left between data privacy laws. The federal uniformity of Swiss data privacy law is a structure any country, particularly a lagging United States, should strive for.

---

[120] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 111–12 (2020).

[121] *Id.*

[122] Council Regulation 2016/679 of Apr. 27, 2016, art. 5, General Data Protection Regulation, 2016 O.J. (L 119) 35–36.

[123] *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 101.

[124] Stauss, *supra* note 116.

[125] *Id.*

[126] Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS., no. 4, 2015, at 231, 235 (discussing Europe's national privacy regulation).

[127] BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101; BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] June 19, 1992, SR 235.1 (1993) *as amended by* Gesetz, Sept. 25, 2020, AS 491 (2022).

1. Ensuring Protection through the Swiss Constitution

Article 13 of the Swiss Constitution guarantees its citizens a right to privacy.[128] In doing so, it establishes that (1) "every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications" and (2) "every person has the right to be protected against the misuse of their personal data."[129] These two short phrases have a greater impact than it seems at first glance. In this regard, the Swiss do not just have a right to their personal data. Rather, they have a greater right to be protected against its misuse.[130]

Article 13 is likely to be a longstanding foundation of the Swiss Constitution. Through its own constitution and the FADP, Switzerland has placed incredible emphasis on data privacy.[131] Upholding these protections, any amendments to Swiss legislation are expressly protected from outside influence.[132] Opinions from citizens and interest groups are only considered during the drafting phase of legislation.[133] Therefore, Article 13 would need to be amended by a majority of voters and cantons (country subdivisions) without outside influence, which would be unprecedented given the country's attention to data privacy.[134] The FADP takes the data privacy baton from the Swiss Constitution across Swiss borders.[135]

2. Addressing Swiss Data Privacy Abroad

Building off Article 13 of the Swiss Constitution, the FADP began protecting data privacy beyond Swiss territory.[136] Addressing cross-border disclosure, Article 6 of the FADP generally requires that personal data be disclosed abroad only if its privacy would not be "seriously endangered"

---

[128] BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101, art. 13.

[129] *Id.*

[130] *Id.*

[131] *See, e.g.*, Amanda Witt & Nicole Beranek Zanon, *Privacy Talk: The New Swiss Data Protection Act*, YOUTUBE (Sept. 10, 2020), https://www.youtube.com/watch?v=Mf8qPEB3ufE.

[132] *See* Michael P. Kunz, *The Influence of Special Interest Groups on Copyright Law and Policy – A Comparison of the Legislative Processes in the United States and Switzerland*, 12 WASH. J.L. TECH. & ARTS 263 (2016).

[133] *Id.* at 51.

[134] Witt & Zanon, *supra* note 131.

[135] BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101, art. 1; BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] June 19, 1992, SR 235.1 (1993), art. 1 *as amended by* Gesetz, Sept. 25, 2020, AS 491 (2022).

[136] BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG] [FEDERAL ACT ON DATA PROTECTION] June 19, 1992, SR 235.1 (1993), arts. 1, 2 *as amended by* Gesetz, Sept. 25, 2020, AS 491 (2022).

due to a lack of legislation that guarantees protection.[137] However, there are still ways to disclose in the absence of such protective legislation. Article 6 details that disclosure would still be possible when (1) sufficient safeguards, particularly in contracts, ensure adequate protection; (2) disclosure is consented to; (3) disclosure is in the performance of a contract; (4) disclosure is essential to uphold public interest or necessary for judicial compulsion; (5) disclosure is required to protect one's life or physical integrity; (6) the data is generally accessible; and (7) disclosure is made between persons under the same company.[138]

While not expressly stated, the purpose of Article 6 of the FADP is to protect the data of Swiss citizens abroad by holding countries to a legislative standard. This standard of serious endangerment is certainly a low one. However, it allows the FADP to step in under circumstances in which other nations' data privacy laws are severely lacking. Absent this safety latch, Swiss citizens' data privacy would be at serious risk in countries that lack adequate protection. Together, the FADP and the Swiss Constitution work tirelessly to protect Swiss data both domestically and internationally.

3. The Future of Swiss Data Privacy with the nFADP

The future of Swiss data privacy law appears strong. Adding to the FADP, the nFADP presents six main changes for businesses. The first three changes redefine the FADP's scope.[139] First, only the data of natural persons, and not those of legal persons, are covered.[140] In other words, aligning with the GDPR, the nFADP only protects the data of persons, not organizations, associations, or foundations.[141] Second, genetic and biometric data are included in the definition of sensitive data.[142] This expands the definition of a "natural person" when they cannot otherwise be uniquely identified.[143] Third, the principles of "privacy by design" and "privacy by default" are introduced.[144] Privacy by design requires that data

---

[137] *Id.* art. 6.
[138] *Id.*
[139] FED. DATA PROT. AND INFO. COMM'R, *supra* note 15, at 3–4.
[140] *Id.* at 3.
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.* at 3–4.

is made anonymous or deleted by default.[145] Privacy by default, on the other hand, requires that private collection of data is restricted to data that is "absolutely necessary for the intended purpose," absent consent.[146] This eliminates the excessive collection of data.

The remaining three changes place security obligations on covered businesses to facilitate data privacy protection.[147] Per the fourth change, businesses with more than 250 employees must actively list all data processing activities.[148] However, this obligation does not extend to federal bodies or businesses whose processing bears a low risk of breach.[149] Fifth, prompt notification to the Federal Data Protection and Information Commissioner is required in the event of a data security breach.[150] Narrowing the GDPR's reporting obligation of any risk, the nFADP only requires the report of breaches that entail high risk of adverse privacy effects or fundamental rights.[151] Finally, Swiss law now controls profiling, or the automated processing of personal data.[152] Private data controllers will have to actively inform data subjects every time personal data is collected.[153]

In making these changes, the nFADP adds pressure to companies wishing to handle Swiss citizens' data. This pressure extends far beyond Swiss borders. The nFADP applies to all processing of personal data that has an effect in Switzerland, even if the process occurs abroad.[154] In doing so, the nFADP keeps a close watch on Swiss citizens' data privacy being handled abroad. Combined with the internal protection of the Swiss Constitution, Swiss citizens can be at ease that their data is carefully protected.

The limited criminal sanctions that the nFADP enforces are necessary to ensure that companies comply with its most important requirements.[155] With its recent implementation, companies hoping to handle Swiss data should ensure that they are compliant with the nFADP because

---

[145] *Id.* at 3.

[146] *Id.*

[147] *Id.* at 5–6.

[148] *Id.* at 5.

[149] *Id.*

[150] *Id.* at 6.

[151] *Id.*

[152] *Id.* at 4.

[153] *Id.* at 5.

[154] Sabrine Schnyder, *A Wakeup Call – The New Swiss Data Protection Act Enters Into Force on September 1, 2023*, SIDLEY AUSTIN (Apr. 2022), https://www.sidley.com/en/insights/publications/2022/04/a-wakeup-call-the-new-swiss-data-protection-act-enters-into-force-on-september-1-2023 [https://perma.cc/T96E-FT6Q].

[155] FED. DATA. PROT. AND INFO. COMM'R, *supra* note 15, at 8.

it does not provide for a transition period.[156] Thankfully, the nFADP should be glorified as an increased protection as opposed to a newborn threat, since full compliance is not required to avoid criminal repercussions. In this regard, its main focus is to protect privacy, as opposed to criminalize business policies.

C. TAKEAWAYS FOR THE UNITED STATES

Switzerland's swift progress in the realm of data privacy law should serve as a lesson for the United States. With the rapid expansion of the internet and the growing accessibility of data, now more than ever is the time for the United States to make serious changes to its data privacy structure. Luckily, Switzerland's handle on data privacy legislation presents three lessons from which the United States can learn: (1) implied constitutional protections are insufficient, (2) strict data privacy laws are attainable, and (3) data privacy protection does not have to end at the border. In taking from these lessons, the United States would be more on par with both Switzerland and the rest of Europe—the leading continent in data privacy.[157]

First, an absence of constitutional protection for data privacy is not an excuse for inadequate data privacy protection. The simple comparison between Switzerland and the United States is that Switzerland has expressed constitutional protection of data privacy, whereas the United States has not. Surely, constitutional safeguards help shield Swiss data privacy, but this is an incomplete explanation of what makes a strong structure. To add to their constitutional provisions, Switzerland has continued to make significant strides in data privacy legislation, beginning with the FADP in 1992 and updating with the nFADP in 2023. Even without Article 13 of the Swiss Constitution, the nFADP comprehensively protects Swiss data privacy beyond its borders.

Second, a world with strict data privacy requirements is attainable. There is no question that Switzerland and the United States stand on opposite ends on the spectrum of data privacy protection. However, this does not tell the full story. Going beyond a country-specific contextual analysis, the European Union has collectively created a data privacy shield with the establishment of the GDPR.[158] Switzerland is not a part of the European

---

[156] Schnyder, *supra* note 154.

[157] Jonathan McGruer, *Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance*, 15 WASH. J.L. TECH. & ARTS 120, 124 (2020).

[158] Rustad & Koenig, *supra* note 8, at 367.

Union but has nonetheless been able to defend its own data.[159] Since the implementation of the FADP, Switzerland has had no need for a widespread bubble such as the GDPR. With their respective protections, both Switzerland and the European Union, accounting for much of Europe, have been successful in holding other countries to a high standard for handling their citizens' data.[160] From its success, Europe has shown that it is both possible and realistic to form a standard of strict data privacy regulation. The United States should be expected to join in Europe's response to growing data privacy threats. The more countries that adopt strict regulations may very well strike a domino effect that leads to widespread data privacy protection.

Third, data privacy protections do not have to be narrowed and defined by borderlines. Switzerland does not stick to its own territory in protecting Swiss data. Doing so would only be a disservice to Swiss citizens, as data is easily transferable across nations with just the click of a button.[161] As this Comment has shown, several state legislatures in the United States do a decent job at addressing their own state's data privacy risks. However, the differences between state laws create headaches of inconsistencies.[162] To resolve inevitable state-by-state differences, a valuable first step would be to create comprehensive federal data privacy protection. A crucial next step, as Switzerland has shown, is to protect US data across borders and overseas. The United States does not have to recreate the wheel in this regard. But it can follow in Switzerland's footsteps by holding countries handling American data to a high regulatory standard, like the nFADP does. Doing so may push other countries to increase their own data privacy protections, helping protect not just American data but also other data the United States handles.

With data privacy under attack, increasing attention must be drawn to different countries' legislative responses. Leading the conversation, Switzerland protects its citizens' data with a close hold in and out of the country through the Swiss Constitution and nFADP. The United States, without explicit constitutional protection or comprehensive law, must learn from the Swiss' quick progress in protecting data privacy.

---

[159] *Countries in the EU and EEA*, GOV.UK, https://www.gov.uk/eu-eea [https://perma.cc/65JA-AE8Y].

[160] *Id.*

[161] Jason Heitz, *Federal Legislation Does Not Sufficiently Protect American Data Privacy*, 49 N. KY. L. REV. 287, 288 (2022).

[162] Citron, *supra* note 80, at 1835.

The United States needs to capitalize on a present and incredible opportunity to catch up with Switzerland and much of Europe. The ADPPA, a comprehensive data privacy bill that has gained the most traction, would significantly reduce the need for state-specific laws and jumpstart the United States' efforts to address data privacy.[163] With the rampant growth of technology and the internet, the time is now for the United States to finally pass a comprehensive data privacy bill. If the ADPPA does not get passed, there is no certainty of when the next comprehensive data privacy bill would enter the conversation. Given the United States' sluggish and polarized legislative process between the House and Senate, the need to pass the ADPPA and not forestall data privacy progress is urgent.[164]

Passing the ADPPA is not the end-all-be-all for the United States. The ADPPA serves many important purposes in strengthening the United States' grip on data privacy. However, its protections stop at the border. With this being the case, the United States must capitalize on passing the ADPPA by creating legislation that reaches beyond its borders. But most importantly, the ADPPA gets the ball rolling for US legislation in furthering progress towards general data privacy.

III. CONCLUSION

Comprehensive data privacy law is critical in a world with sensitive information transmittable with the press of a fingertip. Countries are constantly having to navigate the arising challenges that come with data privacy threats. Analyzing different legislative responses, some countries have firm grips on their citizens' privacy, while others continue to lag. In Switzerland, citizens can be at ease that their data is well protected with constitutional rights and revised legislation that addresses both domestic and foreign threats. In the United States, however, data privacy is extremely vulnerable without comprehensive data privacy legislation. Amending the Constitution to impose data privacy rights is likely too much to ask. But this should not stop Congress from coming to an agreement on a comprehensive bipartisan bill. The ADPPA is an incredible opportunity for Congress. Having gained the most traction out of any

---

[163] Solove, *supra* note 69.

[164] Cynthia R. Farina, *Congressional Polarization: Terminal Constitutional Dysfunction*, 115 COLUM. L. REV. 1689, 1692 (2015).

proposed data privacy bill, it represents the United States' best hope to catch up with Switzerland.