The Business, Entrepreneurship & Tax Law Review

Volume 6 | Issue 2 Article 10

2022

Cross-Border Data Transfers: A Balancing Act through Federal Law

Joshua M. Wilson

Cross-Border Data Transfers: A Balancing Act through Federal Law

Joshua M. Wilson[*]

ABSTRACT

Throughout the digital age, corporations have collected, used, and stored individuals' digital information to efficiently market to consumers and expand their business. In fact, not only do retail companies rely on data, but also farmers, financial institutions, health services, and other businesses heavily depend on one's information. Despite the importance and necessity of data, the U.S. has failed to establish a comprehensive federal law addressing data issues. Many countries with developed or developing economies, however, have established laws related to data, a company's usage of such data, and other data-related issues.

A key obstacle plaguing U.S. businesses in terms of data law is cross-border data transfers. In adopting data-related laws, countries around the world have focused on an individual's right to privacy and strengthened their data privacy regimes. However, because of the lack of a comprehensive federal law, other countries have been cautious or refused to allow U.S. companies to transfer the data of individuals to the United States. This wariness is rooted in the fact that current U.S. data privacy laws do not impose stringent enough standards for businesses that collect and use data, and the belief that the U.S. does not offer adequate protections for an individual's sensitive personal information. Thus, foreign countries bar U.S. businesses from freely transferring data to the United States. As a result, U.S. businesses are required to either incur substantial compliance costs to adhere to foreign standards or cease to do business within countries with stringent data privacy laws.

If the U.S. was to adopt a comprehensive data privacy law, businesses would be able to transfer data freely while protecting an individual's sensitive personal data.

Through looking at data privacy and cross-border data transfers through a comparative law lens, this article proposes that the United States should adopt a comprehensive federal law regarding data privacy. To support this proposal, the article first compares U.S. law to Europe's General Data Protection Regulation ("GDPR") and other countries' laws. This comparative analysis will illustrate how American businesses are disadvantaged by the lack of a general federal law. The comparative analysis also highlights strategies that the U.S. Congress can adopt to strike a better balance to both protect the privacy of U.S. citizens while also allowing U.S. businesses to remain efficient and financially unburdened.

---

[*] J.D. Candidate, University of Missouri School of Law, 2023; B.A. Political Science, B.A. Asian Studies, Minor in Korean & Korean Studies, University of Utah, 2019. I would like to thank Allan Smith, Dana Wiele, and Reinsurance Group of America for giving me an opportunity to work on data privacy-related issues. I would also like to thank my family, friends, and the *Business, Entrepreneurship, & Tax Law Review* for their support while writing this Comment.

I. INTRODUCTION

The term "data" was first used in the 17th century and draws its roots from the Latin word *datum*, meaning "a fact given or granted."[1] From the mid-17th century onward, data was understood to mean "factual information used as a basis for reasoning, discussion, or calculation."[2] As time passed and digital technology emerged, "data" became associated with "transmittable and storable information by which computer operations are performed."[3] At present, "data" is regarded as "information in digital form that can be transmitted or processed."[4] If one ponders the subject, data seemingly penetrates all facets of life.[5] From simply opening digital applications to tracking steps and sending text messages, humans generate substantial amounts of data throughout the course of a day.[6] Regardless of the significance and size of any given piece of digital information, data affects local businesses and international conglomerates,[7] world governments and the electorate,[8] and even individuals living in the most remote parts of the world.[9] For individuals, data influences the type of advertisements that appear in their web browsers or the array of posts they view on their social media feeds.[10] For businesses, digital information affects commercial decisions and assists with supplying goods and services to meet global demand.[11] And for governments, data enables smoother and safer operations by informing leaders of potential dangers and disasters.[12] Producing and receiving data is so vital to our daily lives that humankind would be unable to carry on without it.[13]

The penetration of and dependence on digital information is well illustrated within the business world.[14] Spanning from social security numbers to the shopping habits of consumers, businesses engage with data to create marketing strategies, further develop client experiences, comprehend consumer trends, and, most

1. *Data*, ONLINE ETYMOLOGY DICTIONARY, https://www.etymonline.com/word/data (last updated Oct. 13, 2021).
2. *Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data (last visited Oct. 10, 2022).
3. ONLINE ETMOLOGY DICTIONARY, *supra* note 1.
4. MERRIAM WEBSTER, *supra* note 2.
5. Kathleen Stansberry et al., *Leading Concerns About the Future of Digital Life*, PEW RSCH. CTR. 5 (Oct. 28, 2019), https://www.pewresearch.org/internet/2019/10/28/5-leading-concerns-about-the-future-of-digital-life.
6. Rashi Desai, *Why is DATA Important for Your Business?*, TOWARDS DATA SCI. (Sept. 5, 2019), https://towardsdatascience.com/how-important-is-data-for-your-business-c15a35c6935e.
7. Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last updated Aug. 25, 2022).
8. Kevin Rands, *How Big Data has Changed Politics*, CIO (June 28, 2018, 7:13 AM), https://www.cio.com/article/3285710/how-big-data-has-changed-politics.html.
9. Corianne Payton Scally & Eric Burnstein, *Rural Communities Need Better Data*, URBAN INST. (May 6, 2020), https://www.urban.org/urban-wire/rural-communities-need-better-data.
10. Leslie K. John et al., *Ads That Don't Overstep*, 96 HARV. BUS. REV. 62, 62–63 (2018).
11. Thawipong Anotaisinthawee, *Our Growing Dependence on Data*, BANGKOK POST (June 4, 2019, 4:00 AM), https://www.bangkokpost.com/business/1688960/our-growing-dependence-on-data.
12. *Id.*
13. Andrzej Kawalec, *How Long Could You Survive Without Data?*, VODAFONE LTD., https://www.vodafone.com/business/news-and-insights/blog/gigabit-thinking/how-long-could-you-survive-without-data (last visited Oct. 10, 2022).
14. Anotaisinthawee, *supra* note 11.

importantly, ensure that their business will continue to succeed.[15] In fact, not only do businesses acknowledge their reliance on data but also a majority of businesses admit that it is impractical to do business without digital information.[16]

Due to data's pivotal role in society, the ability of a business to collect, process, store, and transmit digital information of clients, customers, and patients, and the limitations on such abilities dominate data-related issues.[17] To address such issues and create a more secure environment for data, Congress has recently concentrated on drafting legislation that focuses on an entity's ability to collect and use data.[18] Notwithstanding such efforts, the United States has failed to establish a comprehensive federal law related to data privacy and is forced to utilize a murky combination of sector-specific laws to address data privacy and protection issues.[19] The amalgamation of sector-specific laws has led to gaping holes regarding data privacy and created complex challenges for businesses to navigate through as they attempt to piece together relevant laws and resolve data-related matters.[20] To add to the quandary created by sector-specific laws, states have ventured to fill the chasm created by inadequate federal law risk managementby enacting state data protection laws.[21] These state laws, in turn, cause more confusion and perplexity.[22]

The absence of a comprehensive data privacy standard is unsustainable because the deficiency adversely affects regional, domestic, and international business.[23] Not only are U.S. consumers at risk of harm due to the absence of federal data privacy law,[24] but also local, domestic, and international companies are significantly disadvantaged in terms of risk-management, foreign trade, and global competitiveness.[25] Therefore, this article proposes that the United States should adopt a comprehensive federal law regarding data privacy. To support this proposal, the article first compares U.S. law to Europe's General Data Protection Regulation ("GDPR") and other countries' laws. This comparative analysis will illustrate how American businesses are disadvantaged by the lack of general federal law. The comparative analysis also highlights strategies that the U.S. Congress can adopt to strike a better balance to both protect the privacy of U.S. citizens while also allowing U.S. businesses to remain efficient and financially unburdened.

---

15. *See id.*

16. Jay Leonard, *Over 50% of Businesses State They Can't Survive without Quality Data*, BUS. 2 CMTY., https://www.business2community.com/big-data/over-50-of-businesses-state-they-cant-survive-without-quality-data-02237820 (last updated Sept. 9, 2019).

17. Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data.

18. *Data Privacy Laws: What You Need to Know in 2022*, OSANO, https://www.osano.com/articles/data-privacy-laws (last updated July 4, 2022).

19. *Id.*

20. *See* Chakravorti, *supra* note 17.

21. OSANO, *supra* note 18; Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us.

22. *Id.*

23. Owen McCoy, *A Legislative Comparison: US vs. EU on Data Privacy*, EDAA, https://edaa.eu/a-legislative-comparison-us-vs-eu-on-data-privacy (last visited Oct. 10, 2022). *See also* Joanna Redden, Jessica Brand and Vanesa Terzieva, *Data Harm Record (Updated)*, DATA JUSTICE LAB, https://datajusticelab.org/data-harm-record (last updated Aug. 2020).

24. *See* discussion *infra* Part IX.

25. *See* Letters from CEOs, Business Roundtable CEOs, to Congress (Sept. 10, 2019), https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-Finalv2.pdf.

II. DATA: PROTECTION, PRIVACY, AND SECURITY

In this digital age, data is information recorded in any form or medium that can be digitally collected, processed, and transmitted.[26] Data is constantly generated throughout the world.[27] Americans use approximately 4.4 million Gigabytes of data per minute.[28] In 2020, the world generated 64.2 zettabytes (6.42×10^{22} bytes or 64.2 trillion Gigabytes) worth of data.[29] By 2025, data experts forecast that global data creation will exceed 180 zettabytes.[30] While individuals generate data through frequent internet use, accepting cookies, and storing crucial personal information with businesses, companies collect data to refine their marketing strategies and generate cash flow, and advertising.[31]

Multinational corporations like Apple, Facebook, and Google collect and maintain access to some of our most personal information.[32] These companies request and gather vital details related to our image and voice, access our image libraries and credit card information, and may even know our weight and blood type. [33] The general consumer tends to view the collection and storage of one's personal data as non-intruding and beneficial because it enables one-click shopping, finding products more efficiently, and increasing global cooperation to instill innovation; however, data collection and storage carry massive negative implications.[34] As a result of mass data compiling by companies, information is consolidated at one location and becomes easily accessible.[35] If such data is breached or leaked, an individual can suffer great financial, physical, or psychological damage, among other consequences.[36]

A data breach is "[t]he loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence was (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for" an

26. MERRIAM WEBSTER, *supra* note 2; PRINCIPLES OF THE L. OF DATA PRIVACY § 2(a) (AM. L. INST 2020).

27. Nicole Martin, *How Much Data Is Collected Every Minute Of The Day*, FORBES (Aug. 7, 2019, 03:34 PM), https://www.forbes.com/sites/nicolemartin1/2019/08/07/how-much-data-is-collected-every-minute-of-the-day/?sh=4e0a6b593d66; Matt Gaedke, *How Much Data is Generated Every Minute on the Minute*, DAILY INFOGRAPHIC (Dec. 1, 2021), https://dailyinfographic.com/how-much-data-is-generated-every-minute.

28. *Id.*

29. *The World Generated 64.2 Zettabytes of Data Last Year – But Where Did it All Go?*, TECHDAY (Mar. 26, 2021), https://datacenternews.asia/story/the-world-generated-64-2-zettabytes-of-data-last-year-but-where-did-it-all-go.

30. *Amount of Data Created, Consumed, and Stored 2010-2025*, STATISTA (Sept. 8, 2022), https://www.statista.com/statistics/871513/worldwide-data-created.

31. Freedman, *supra* note 7.

32. Andriy Slynchuk, *Big Brother Brands Report: Which Companies Might Access Our Personal Data the Most?*, CLARIO: BLOG, https://clario.co/blog/which-company-uses-most-data (last updated July 22, 2021).

33. *Id.*

34. *See* Tashina Alavi, *4 Benefits You Receive by Sharing Your Data to Companies*, TOWARDS DATA SCI. (Nov. 30, 2020), https://towardsdatascience.com/4-benefits-you-receive-by-sharing-your-data-to-companies-70ca58e11989.

35. Bill Toulas, *Over 20,000 data center management systems exposed to hackers*, BLEEPING COMPUT. (Jan. 29, 2022), https://www.bleepingcomputer.com/news/security/over-20-000-data-center-management-systems-exposed-to-hackers.

36. *Personal Data Breaches*, ENISA, https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches (last visited Nov. 5, 2021).

unauthorized purpose.[37] Data is crucial to one's identity and breaches subject consumers to widespread harm.[38] While breaches vary in size and effect, the threat they pose to an individual's data is illuminated by understanding that 45% of U.S. companies experienced a data breach in 2020, and 65% of U.S. companies experienced data breaches in 2019.[39] A cyberattack on data happens less than every 39 seconds,[40] and the average user's chance of having data compromised is 27.9%.[41] By way of further illustration, some key incidents related to data breaches include Yahoo's data breach in 2013, Alibaba's breach in 2019, and LinkedIn's breach in 2021.[42] These incidents alone affected a total of 5 billion individuals worldwide.[43] Due to these breaches, users of services like Yahoo and LinkedIn have become the target of spam campaigns and victims of identity theft.[44]

Three key areas related to the scope and ability of a company to collect, store and transmit data, and prevent breaches are data privacy, protection, and security.[45] Data protection is the concept of ensuring that data remains in the correct hands and "the process of safeguarding important information from corruption, compromise or loss."[46] Data security acts as an extension of data protection: it encompasses a company's measures to back-up information, retain data, monitor threats, and encrypt such information to prevent data loss.[47] Such actions ensure that sensitive data is protected, and external and internal threats are minimized.[48]

Meanwhile, data privacy is not clearly defined like its counterparts of protection and security.[49] Data privacy stems from the principle of a right to privacy, which is often defined as an individual's right "to be let alone."[50] As digital information emerged, and the concept of the right to privacy extended to data, data privacy has come to be defined broadly to refer to privacy laws that "regulate various

37. U.S. DEP'T OF JUST., REPORTING AND RESPONSE PROCEDURES FOR A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2018).

38. Paige Schaffer, *Data Breaches' Impact on Consumers,* INS. THOUGHT LEADERSHIP (July 29, 2021), https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

39. Aimee O'Driscoll, *30+ Data Breach Statistics and Facts*, COMPARITECH , https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts (last updated Sept. 16, 2022).

40. Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, UNIV. OF MD. SCH. OF ENG'G (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

41. Randy Lindberg, *Data Breach Statistics to Know for 2021*, RIVAL DATA SEC. (Nov. 16, 2020), https://www.rivialsecurity.com/blog/data-breach-statistics.

42. Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (July 16, 2021, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

43. *Id*.

44. *See* Tara Seals, *Data for 700M LinkedIn Users Posted for Sale in Cyber-Underground*, THREATPOST (June 28, 2021, 7:24 PM), https://threatpost.com/data-700m-linkedin-users-cyber-underground/167362/#:~:text=%E2%80%9CThe%20leaked%20information%20poses%20a,%2C%20victims%20of%20identity%20theft.%E2%80%9D.

45. Brien Posey, *Comparing Data Protection vs. Data Security vs. Data Privacy*, TECHTARGET (Feb. 2, 2021), https://searchdatabackup.techtarget.com/tip/Comparing-data-protection-vs-data-security-vs-data-privacy.

46. *What is Data Protection?*, SNIA, https://www.snia.org/education/what-is-data-protection (last visited Nov. 5, 2021).

47. *Id.*

48. *Id.*

49. *Id.*

50. *See* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed., Chicago, Callahan & Company 1888); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

aspects of the collection, use, processing, storage, and disclosure of all" personal information.[51]

Ultimately, the objective of each area is the same because each looks to ensure that an individual's data remains safe and immutable within corporate servers and while corporations conduct business.[52]

III. THE ROLE OF DATA PRIVACY AND ITS EFFECT WITHIN THE UNITED STATES

Data privacy laws encompass the collection, processing, use, storage, and transmission of personal data.[53] Generally, "personal data" is "any data regarding an individual, including, but not limited to personal identifiers."[54]

Personal data can be separated into three categories: sensitive/confidential personal data, general personal data, and details of criminal offenses.[55] Notwithstanding such categorization, the extent of what is considered sensitive and general personal data differs based on where one resides.[56] Sensitive personal data typically encompasses information related to an individual's personal health, finances, creditworthiness, biometric data, and details that can be used to perform identity theft or fraud.[57] On the other hand, general personal data encompasses anything not included within the scope of sensitive personal data.[58] Privacy laws seek to regulate both sensitive and general personal data to enhance trust in business, seamless electronic transfers across borders, and prevent any data from being misused by third parties for fraud.[59]

Notwithstanding its importance, the U.S. federal government has failed to enact a comprehensive federal law related to businesses protecting general and sensitive personal information.[60] Instead, the U.S. has attempted to resolve data privacy issues by establishing guidelines for government agencies and protecting "personally identifiable information" ("PII").[61] PII can be both sensitive and general personal data.[62] PII is data that can be used to extract and ascertain an individual's identity,

51. Brian M. Gaff et al., *Privacy and Data Security*, 45 IEEE COMPUT. SOC'Y 8, 8 (2012).

52. PRINCIPLES OF THE L. OF DATA PRIVACY § 1 (AM. L. INST 2020).

53. *Id.*

54. Brossard v. Univ. of Mass., 1998 WL 1184124, at *8 (Mass. Super. Sept. 29, 1998). *See also* Organisation for Economic Co-operation and Development [OECD], *Recommendations of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, at 5, OCED/LEGAL/0188 (Sept. 9, 1980) ("[p]ersonal data" means "any information relating to an identified or identifiable individual (data subject)").

55. *Types of Personal Data*, AARHUS UNIV., https://medarbejdere.au.dk/en/informationsecurity/data-protection/general-information/types-of-personal-data (last visited Oct. 11, 2022).

56. *Definition of Personal Data*, DLA PIPER, https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US (last modified Jan. 24, 2022)

57. *Definition of Personal Data*, *supra* note 56.

58. *Id.*

59. *Why is Data Protection so Important*, FSB: BLOGS (May 13, 2021), https://www.fsb.org.uk/resources-page/why-is-data-protection-so-important.html.

60. *Data Privacy Principles All Legal Providers Should Adopt*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/data-privacy-principles (last visited Oct. 11, 2022).

61. RAYMOND T. NIMMER & HLLY K. TOWLE, DATA PRIVACY, PROTECTION, AND SECURITY LAW § 2.01 (LexisNexis A.S. Pratt 2022); U.S. DEP'T OF COM., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995).

62. Jake Frankenfield, *Personally Identifiable Information (PII)*, INVESTOPEDIA, https://www.investopedia.com/terms/p/personally-identifiable-information-

either by itself or by combining "other personal or identifying information that is linked or linkable to a specific individual."[63]

To protect PII collected and utilized by the U.S. government, the U.S. has adopted internal directives and guidelines for police government agencies and established rules regarding handling PII.[64] However, the scope of these directives and guidelines only applies to contractors of government agencies and the agencies themselves.[65] In addition to directives, the U.S. attempted to address data privacy within the U.S. by enacting the Privacy Act of 1974.[66] The Privacy Act of 1974 operates under the mission to "balance the government's need to maintain information about individuals with the rights of the individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information."[67] The issue with the Privacy Act, however, is that it applies to the government, and not private parties and individuals, much like the directives and guidelines established by various U.S. government agencies.[68] And because the Privacy Act does not extend to businesses, the extent to which businesses must protect data after a business collects digital information is unregulated by a single U.S. federal law.[69]

Despite the Privacy Act's limited reach around a private business's data protection efforts, the U.S. government has previously attempted to regulate businesses and protect PII and data through the efforts of the Federal Trade Commission ("FTC").[70] The FTC is considered to be the entity that has the power to establish a national framework for data privacy.[71] Established by the FTC Act, the Commission can take measures against persons, partnerships, or corporations to prevent unfair methods of competition, and any actions that affect commerce using unfair or deceptive acts.[72] Using such powers, the FTC took an active role in issues of online privacy and addressed data privacy issues in the 1990s.[73] Yet, after the early 2000s, this fire seemingly extinguished and the FTC has not moved on data privacy issues recently despite holding broad enforcement powers.[74]

---

pii.asp#:~:text=Personally%20identifiable%20information%20(PII)%20can,Social%20Security%20Number%20(SSN) (last updated Feb. 25, 2022).

63. Memorandum From Peter R. Orszag on Guidance for Agency Use of Third-Party Websites and Applications to the Heads of Executive Departments and Agencies (June 25, 2010).

64. GEN. SERVS. ADMIN., CIO 2180.2, GSA RULES OF BEHAVIOR FOR HANDLING PERSONALLY IDENTIFIABLE INFORMATION (PII) (2019); *Guidance on the Protection of Personal Identifiable Information*, U.S. DEP'T OF LAB., https://www.dol.gov/general/ppii (last visited Nov. 20, 2022); *Personally Identifiable Information (PII)*, U.S. DEP'T OF ENERGY, https://www.directives.doe.gov/terms_definitions/personally-identifiable-information-pii (last visited Nov. 20, 2022); U.S. DEP'T OF HOMELAND SEC., DHS PRIVACY POLICY DIRECTIVE 047-01-007, REVISION 3, HANDBOOK FOR SAFEGUARDING SENSITIVE PII (2017).

65. *See* sources cited *supra* note 64 and accompanying text.

66. 5 U.S.C. § 552(a).

67. *Overview of the Privacy Act of 1974*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/opcl/policy-objectives (last visited Nov. 5, 2021).

68. *See* U.S. DEPT. OF JUST. *supra* note 67.

69. *Data Privacy Principles All Legal Providers Should Adopt*, *supra* note 60.

70. *What the FTC Could Be Doing (But Isn't) To Protect Privacy*, ELEC. PRIV. INFO. CTR., https://epic.org/wp-content/uploads/2021/10/EPIC-FTC-Unused-Authorities-Report-June2021.pdf (last visited Sept. 26, 2022); *Federal Trade Commission Act*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (last visited Apr. 26, 2022); 15 U.S.C. §§ 45–58.

71. *See* sources cited *supra* note 70 and accompanying text.

72. §§ 45–58.

73. *What the FTC Could Be Doing (But Isn't) To Protect Privacy*, *supra* note 70.

74. *Id.*

The U.S. has managed to avoid establishing a comprehensive federal standard by creating sector-specific laws that deal with areas like telecommunications, financial institutions, credit information, and social media.[75] As a result of the complex mixture of sector-specific laws, individuals domestically and internationally describe U.S. data privacy law as a "cluttered mess of different sectoral rules."[76] A few federal laws that address various concepts of data privacy are the Health Insurance Portability and Accountability Act ("HIPAA"), which addresses the collection of health information, the Fair Credit Reporting Act ("FCRA"), and the Gramm-Leach-Bliley Act ("GLBA"), which govern financial and credit information, and the Family Educational Rights and Privacy Act ("FERPA") and Children's Online Privacy Protection Act ("COPPA"), which address information concerning children and educational rights.[77]

While each law has its strengths regarding data privacy, all lack the necessary requirements to ensure that data remains secure while corporations collect, maintain, and transfer personal information.[78] For example, the FCRA was the first federal law to regulate the use of personal information by private businesses and was enacted to promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies ("CRAs").[79] The law establishes disclosure requirements for businesses when a client suspects identity fraud[80] and enumerates other obligations for entities, such as requiring CRAs to maintain procedures to guarantee that personal information is protected and accurate.[81] Even with these requirements, personal information is often mixed with other individuals' information and is inaccurate, which causes Americans to be denied credit, suffer embarrassment, or have their identities stolen.[82] Furthermore, the FRCA enables anyone with a "legitimate business need" to obtain consumer reports and offers a broad loophole for any business to receive sensitive personal and financial information.[83] Consequently, an individual's sensitive credit information is not thoroughly protected because all businesses can potentially claim that they have a "legitimate business need" and obtain a data subject's information with ease.[84] Finally, the FCRA lacks requirements related to transparency when consumer data is leaked, and instead allows CRAs to lie low until a data subject requests to know about a breach regarding their credit information.[85]

75. OSANO, *supra* note 18.

76. Klosowski, *supra* note 21.

77. OSANO, *supra* note 18. *See also* 42 U.S.C. §§ 1320d(1)–(9); 15 U.S.C. 1681 et seq., 15 U.S.C. § 6801 et seq., 20 U.S.C. § 1232g; 15 U.S.C. § 6501 et seq.

78. Daniel Solove, *HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry,* AHIMA (Apr. 2013), https://bok.ahima.org/doc?oid=106326#.Yk_JES-B2Cg.

79. 15 U.S.C. § 1681; *The Fair Credit Reporting Act (FRCA)*, EPIC, https://epic.org/the-fair-credit-reporting-act-fcra-and-the-privacy-of-your-credit-report (last visited Oct. 11, 2022).

80. § 1681c-1.

81. § 1681e.

82. Spokeo v. Robins 578 U.S.C. 330, 353-54 (2016); Albert S. Jacquez & Amy S. Friend, *The Fair Credit Reporting Act: Is It Fair for Consumers?*, 5 LOY. CONSUMER L. REV. 81, 83 (1993); David Anthony et al., *CFPB Settlement Shows Common FCRA Compliance Flaws*, TROUTMAN PEPPER HAMILTON SANDERS LLP. (Nov. 30, 2020), https://www.troutman.com/images/content/2/7/272598/2020-11-30-Law360-CFPB-Settlement-Shows-Common-FCRA-Complian.pdf.

83. Jacquez & Friend, *supra* note 82.

84. Solove, *supra* note 78.

85. *See* David Anthony & Julie Hoffmeister, *FRCA May Be a Dead End for Data Breach Plaintiffs*, TROUTMAN PEPPER HAMILTON SANDERS LLP (Jan. 28, 2016), https://www.troutman.com/insights/fcra-may-be-a-dead-end-for-data-breach-plaintiffs.html.

While one would think that financial information should be extensively protected, not only does the FCRA fall short in protecting data, but also the GLBA, which regulates financial institutions and information, provides minimal protection for financial data. [86] At first glance, the GLBA seemingly provides broad oversight and protection of data because it imposes privacy requirements when financial institutions collect "nonpublic personal information about individuals who obtain financial products or services."[87] However, regulations on data are only imposed when an individual obtains financial products or services primarily for "personal, family or household purposes."[88] In other words, the GLBA does not provide protection for individuals when an individual obtains "financial products or services for business, commercial, or agricultural use" and the financial institution collects sensitive personal information.[89] Thus, if an individual were to apply to a bank to open a sole proprietorship business account with their social security number, the individual's data would be at risk. Therefore, financial institutions have immense control over the collection, processing, and transfer of information for individuals that obtain financial products for business and are essentially unregulated in terms of protecting a data subject's personal information.[90]

Even the United States' most thorough data privacy law fails to adequately protect individuals' data.[91] HIPAA provides a national data privacy framework for businesses that deal with health-related information.[92] It requires businesses dealing with personal health information ("PHI") to implement administrative, physical, and organizational safeguards to ensure confidentiality and protect against breaches.[93] While HIPAA establishes thorough restrictions to ensure that the most sensitive personal information (health information) is protected, HIPAA fails because it does not extend to all individuals and institutions that collect, obtain, maintain, and disclose individually identifiable health information.[94] Furthermore, it falls short of providing adequate data protection because the U.S. Department of Health and Human Services ("HHS") often does not enforce HIPAA regulations against institutions that violate privacy rules.[95]

Because of the severe gaps in federal law, some states have endeavored to enact their own laws to protect individuals' data.[96] As of November 2022, five states within the U.S. have adopted a comprehensive consumer privacy law.[97] These laws differ in regard to the restrictions and rules that businesses must adhere to in order

86. David Zetoony, *Financial institution confusion: Are financial institutions fully exempt from the CCPA, CPRA, VCDPA, and CPA?*, NAT. L. REV. (July 2, 2021), https://www.natlawreview.com/article/financial-institution-confusion-are-financial-institutions-fully-exempt-ccpa-cpra.

87. *Id.*; 16 C.F.R.§ 313.1(b) (2022).

88. Zetoony, *supra* note 86.

89. *Id.*

90. *See id.*

91. Solove, *supra* note 78.

92. 45 C.F.R. § 164.104 (2013).

93. §§ 164.308, 164.310(c), 164.314.

94. Stacey Tovino, *HIPAA's Strengths and Limitations*, THE REG. REV. (Aug. 20, 2021), https://www.theregreview.org/2021/08/20/tovino-hipaa-strengths-and-limitations.

95. *Disadvantages of HIPAA*, FIN. WEB, https://www.finweb.com/insurance/5-disadvantages-of-hipaa.html (last visited Apr. 10, 2022).

96. Klosowski, *supra* note 21.

97. *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.

to continue to collect and maintain data and transfer it elsewhere.[98] Most importantly, these state laws differ in strength in regard to data collection and sharing rights, opt-in consent, data minimization, and non-discrimination.[99] In turn, these differences cause businesses to leave certain marketplaces due to additional data privacy-related costs and inhibit economic growth within certain states.[100]

Naturally, the cluttered mess of data privacy laws and the lack of a comprehensive standard within the U.S. leads to boundless domestic issues.[101] In particular, despite the efforts by states to fill the legislative hole in terms of federal data privacy regulation, a state-by-state approach is inherently problematic. From a consumer's perspective, discussions within state legislatures allow corporations to meddle with the law-making process through lobbying and lead to less protective data standards.[102] The adoption of a federal standard would help combat this problem as key businesses in each industry could lobby alongside consumer data privacy groups to create a coherent and equal law.

From a business standpoint, the state-by-state approach is troublesome because businesses looking to do business in other states will have to accommodate and adapt to widely different sets of legal rules governing data privacy.[103] For example, issues may arise regarding whether businesses are liable for not offering opt-out consents to consumers within a certain state. If a business's website adheres to less strict data privacy laws provided by the state the business is incorporated in, and the consumer accesses the website from a state with strict data privacy standards and inputs information into the business's interface, issues would certainly arise. A state-by-state approach creates significant compliance costs for businesses and confusion for consumers in addition to raising costs for out-of-state businesses.[104] As a result, businesses will find themselves subject to a sea of similar-yet-different sets of laws.

This approach also generates massive market inefficiency and deters small businesses from expanding into other markets.[105] The Information Technology and Innovation Foundation ("ITIF") predicts that over the next several years restrictive privacy regulations could generate $104 billion in market inefficiencies for businesses which would lead to businesses operating at lower productivity.[106] This would thwart innovation within the marketplace and cause companies to offer services and products for higher costs and burden consumers.[107] This shift would cause small businesses to bear a substantial burden as they would pay approximately 20 to 23 billion dollars to comply with individual state data privacy requirements, and would consequently be deterred from expanding into other markets.[108] Other legal challenges that arise from the state-by-state approach relate to due process, ample

98. *Id.*
99. *Id.*
100. Daniel Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws*, ITIF (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.
101. Carsten Rhod Gregersen, *The US Is Leaving Data Privacy to the States—and That's a Problem*, MARSH MCLENNAN (Aug. 19, 2019), https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem.
102. *Id.*
103. *Id.*
104. Castro et al., *supra* note 100.
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*

contacts for a business within a territory,[109] lack of standing,[110] and the unjust application of secondary liability on businesses.[111]

Between the complex mesh of federal data privacy laws and the wave of state data privacy laws being considered, adopting a comprehensive federal law would play a pivotal role in shaping fair and equal data privacy laws that maximize protection for consumers while enabling businesses to operate efficiently and with less detriment to economic and technological growth.[112]

IV. THE EU GENERAL DATA PROTECTION REGULATION

In a continually globalizing society, data privacy is not only key to domestic business, but also international trade.[113] Unfortunately, the global community recognizes that U.S. data privacy law offers inadequate protection for data subjects which has impeded American corporations from maximizing revenue and growth in an international business environment.[114] Internationally, the standard for data privacy is set by the European Union ("EU").[115] The EU provides an international framework for data privacy through the EU General Data Protection Regulation ("GDPR").[116]

The GDPR is a set of rules that applies to companies in all sectors which defines how organizations and companies are required to use personal data to ensure that data subject rights are not infringed.[117] In protecting data subject rights, the GPDR establishes regulations on how organizations process data and defines processing as "any operation . . . which is performed on personal data . . . such as collection, recording, organization, structuring, [and] storage."[118]

In accordance with standards set by the GDPR, organizations must use personal data legally, in line with integrity-friendly principles, and in a respectful manner to

109. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (ruling that due process requires that an individual have certain minimum contacts within the applicable territory of forum to not offend 'traditional notions of fair play and substantial justice.').

110. *See* Ouachita v. Wilson, 43,193, p. 7–8 (La. App. 2 Cir. 4/30/08; 981 So. 2d 246, 250–51); Healthtek Solutions, inc. v. Fortis Bens. Ins. Co., 274 F. Supp. 2d 767, 778 (E.D. Va. 2003); Chen v. Zak, No. 3.18-cv-00283, 2020 WL 127645, at *5 (M. D. Tenn. Jan. 10, 2020).

111. SoderVick v. Parkview Health Sys., Inc., 148 N.E.3d 1124, 1125–29 (Ind. Ct. App. 2020).

112. Makenzie Holland, *Federal data privacy legislation could benefit U.S. economy,* TECHTARGET (June 14, 2021), https://www.techtarget.com/searchcio/news/252502418/Federal-data-privacy-legislation-could-benefit-US-economy.

113. *See* United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Regulations and International Data Flows: Implications for Trade and Development*, UNCTAD/WEB/DTL/STICT/2016/1/iPub (Apr. 2016).

114. Justin Sherman, *Weak US Privacy Law Hurts America's Global Standing*, WIRED (July 20, 2021), https://www.wired.com/story/weak-us-privacy-law-hurts-americas-global-standing; 杉本 武重 [Takeshige Sugimoto], 対応急務！ 米国の個人情報保護政策に待ったなし [*Urgent Response! No Waiting for the U.S. Personal Information Protection Policy*], D-COM (July 15, 2021), https://project.nikkeibp.co.jp/decom/atcl/070800017/070800001.

115. *European Union – Data Privacy and Protection*, INT'L TRADE ADMIN., https://www.trade.gov/european-union-data-privacy-and-protection (last visited Oct. 10, 2022).

116. *Id.*

117. *GDPR Summary*, GDPR SUMMARY, https://www.gdprsummary.com/gdpr-summary (last visited Oct. 10, 2022).

118. Council Directive 2016/679 of Apr. 27, 2016, General Data Protection Regulation, art. 4(2), 2016 O.J. (L 119) 1, 33 [hereinafter GDPR]. Council Directive 2016/679 of Apr. 27, 2016, General Data Protection Regulation [hereinafter GDPR], art. 4(2), 2016 O.J. (L 119) 1, 33.

human rights.[119] Therefore, organizations must have a legitimate purpose to collect data, and all data should be collected and processed minimally and only when absolutely necessary.[120] Moreover, the GDPR lays out standards regarding keeping personal data accurate, holding data for a specified length of time, ensuring data security through technical measures, and obtaining consent from a data subject to process their data.[121] When personal data breaches arise, organizations are required to report breaches to data subjects within 72 hours.[122] To ensure that organizations comply with the GDPR, organizations that violate the law may face sanctions up to the amount of 4% of their global sales or 20 million euros.[123]

Strict data privacy regulation provided by the GDPR benefits the EU as it promotes better data hygiene, cybersecurity, and trust between corporations and individuals.[124] Through compliance, corporations grasp a better understanding of the data being collected and focus time, effort, and money on improved data management.[125] Also, due to strict standards, compliance under the GDPR means that businesses need to know precisely what sensitive information they hold onto.[126] In turn, businesses seek to audit the data they possess and implement mechanisms to make data easily accessible to authorized personnel.[127] Adherence to GDPR standards thus enables better cybersecurity and data hygiene as businesses understand how data is used and how to minimize unnecessary data collection.[128] Trust and credibility between clients and businesses also grow as organizations demonstrate that they can follow GDPR standards. [129] Many Europeans believe that lawfulness, transparency, data minimization, and other principles are pivotal to protecting their sensitive personal information.[130]

To further enhance trust between businesses and data subjects, the GDPR mandates that a business obtain consent from data subjects before collecting and using their personal data.[131] Obtaining consent enables people to control their own data without having to worry about the extent to which a company will use their sensitive data.[132] As a result, consent paves the way for transparency about how data is used

---

119. GDPR SUMMARY, *supra* note 117.
120. GDPR, *supra* note 118, art. 5(1), 2016 O.J. (L 119) 35-36.
121. *Id.* at art. 33(1), 2016 O.J. (L 119) 52. *See also* Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR EU, https://gdpr.eu/what-is-gdpr (last visited, Nov. 5, 2021).
122. GDPR SUMMARY, *supra* note 117.
123. *Id.*
124. Tim Mullahy, *A New Era of Privacy—Why Regulations like the GDPR Are Actually a Good Thing for Your Business*, CPO MAGAZINE (Jan. 16, 2019), https://www.cpomagazine.com/data-protection/a-new-era-of-privacy-why-regulations-like-the-gdpr-are-actually-a-good-thing-for-your-business.
125. Harry Hanelt, *GDPR: A Strategic Opportunity*, FORBES (June 25, 2020, 8:20 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2020/06/25/gdpr-a-strategic-opportunity/?sh=1128757937bc.
126. Michael Fimin, *Five Benefits GDPR Compliance Will Bring to Your Business*, FORBES (Mar. 29, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/?sh=615cbdc3482f.
127. *Id.*
128. *Id.*
129. John Edwards, *6 Business Benefits of Data Protection and GDPR Compliance*, TECHTARGET (Jan. 14, 2021), https://searchdatabackup.techtarget.com/tip/6-business-benefits-of-data-protection-and-GDPR-compliance.
130. *Id.*
131. John Marshall, *GDPR: An Opportunity to Build Trust*, GROVO: BLOG, https://blog.grovo.com/gdpr-builds-customer-trust (last visited Oct. 10, 2022).
132. *Id.*

and frees individuals from the harmful effects of automated decision-making.[133] Another key effect of consent and transparency is that clients are more likely to trust organizations and their operations, and frequently use such entities because of the rapport that has been built through complying with data privacy standards.[134]

Despite the benefits that the GDPR affords data subjects around Europe and the world, corporations within the U.S. believe that a GDPR-like data privacy law would be detrimental to the country and their companies.[135] Individuals often cite cultural differences between Europe and the U.S., varying aims of data privacy legislation, the lack of administrative power to enforce GDPR-like data privacy laws, and a lack of corporate and public demand as reasons why a similar law would fail in implementation.[136] Another problem with the GDPR is the amount of time and money it takes for a business to set up facilities and procedures to comply with the standard.[137]

However, a GDPR-like federal law would work in the U.S. as consumers desire greater protection and because U.S. businesses already interact with clients globally including data subjects that reside in GDPR-subjected areas.[138] Consumers have expressed a desire for greater data protection through participating in various studies and surveys where they have expressed that they would be willing to invest time and money to better protect their privacy.[139] This sentiment has also been evidenced in practice as a CMO Council study found that businesses who have complied with the GDPR have seen better engagement from consumers.[140] Furthermore, even though the GDPR requires continual compliance and demands that businesses spend money to comply with its requirements, this is a smaller issue than conflated.[141] Because of the U.S.'s lack of a current federal data privacy law, the U.S. can easily consider the weaknesses of the GDPR and create a GDPR-like data privacy law that ensures that data subjects are protected while being mindful of small business as to not financially burden them as sharply as the GDPR.

---

133. *Id.*

134. Rob Eleveld, *Embracing GDPR And CCPA To Build Consumer Trust*, FORBES (Nov. 15, 2019, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2019/11/15/embracing-gdpr-and-ccpa-to-build-consumer-trust/?sh=2ff7161b7951.

135. Tim Lahan, *Why Europe's GDPR Magic Will Never Work in the US*, WIRED (Feb. 2, 2020, 6:00 AM), https://www.wired.co.uk/article/us-version-gdpr.

136. *Id.*; Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83.

137. Marin Perez, *GDPR Compliance and Small Business*, MICROSOFT (Mar. 28, 2019), https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/gdpr-compliance-and-small-business.

138. *Id.*

139. *New Study Shows Consumers Want to Protect Data Privacy*, IAPP (Oct. 4, 2021), https://iapp.org/news/a/new-cisco-study-emphasizes-consumer-mistrust-in-ai.

140. *See* Perez, *supra* note 137; *GDPR: Impact and Opportunity*, CMO COUNCIL, https://www.cmocouncil.org/thought-leadership/reports/gdpr-impact-and-opportunity (last visited Oct. 10, 2022).

141. Jennifer Huddleston, *The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More*, AM. ACTION F. (June 3, 2021), https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more.

V. THE KEY ISSUE WITH THE LACK OF U.S. DATA PRIVACY LAW: CROSS-BORDER TRANSFERS

Notwithstanding current mechanisms attempting to address data privacy, a significant obstacle facing U.S. companies in terms of data privacy is GDPR compliance and the global trend of governments preferring data localization.[142] Because the GDPR not only applies to European entities but also applies to any global entity that conducts business or interacts with data from the EU, the GDPR is recognized as key law concerning data privacy and protection around the world.[143] Accordingly, the U.S. and other jurisdictions recognize and follow trends set by the European Commission and the GDPR.[144] The U.S., for example, has recognized the GDPR through its courts and has stated that the GDPR is a comprehensive data privacy standard for the European Union.[145] Courts have stated, "the GDPR concerns the data protection and privacy of all EU citizens and regulates the transfer of EU citizens' personal data outside of EU member states, such as the transfer to the U.S."[146] While U.S. courts are not bound by the GDPR, U.S. courts construe the GDPR as an objection by a foreign state seeking to protect its residents and thus courts afford comity towards individuals or nation states that consider the GDPR.[147]

In a continually globalizing market, data privacy issues turn to differences in data privacy laws and focus on a corporation's ability to transfer data overseas.[148] The sheer number of individuals using the internet demonstrates that data circulates globally.[149] With the constant usage of the internet, information moves across national borders and drives the global economy.[150] Cross-border data transfers also enable both large and small businesses to access reliable data to meet international demand, maintain supply chains, and service clients around the world.[151] In turn, small and medium-sized corporations that access the global supply chain and rely on data transfers have seen a 22% increase in revenue in comparison to those that do not.[152] Additionally, as e-commerce grows, investors are attracted to global companies, and businesses looking to expand into global marks employ more individuals to help sustain their international operations.[153] In turn, GDP for countries

142. Mike Swift, *Data Localization Accelerates Globally as Privacy is Linked with Data Transfer Restrictions*, MLEX (May 5, 2021), https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/data-localization-accelerates-globally-as-privacy-is-linked-with-data-transfer-restrictions.
143. Hanelt, *supra* note 125.
144. Phillips v. Vesuvius USA Corp., 2020-Ohio-3285 at ¶¶ 22–23. *See also* Dan Simmons, *13 Countries with GDPR-like Data Privacy Laws*, COMFORTE INC. (Jan. 12, 2021), https://insights.comforte.com/13-countries-with-gdpr-like-data-privacy-laws.
145. *Phillips*, 2020-Ohio at ¶¶ 22–23.
146. *Id. See also In re* Mercedes-Benz Emissions Litig., No. 2:16-cv-881 (KM) (ESK), 2020 WL 103975, at *1 (D.N.J. Jan. 30, 2020).
147. AnywhereCommerce, Inc. v. Ingenico, Inc., No. 19-CV-11457-IT, 2020 WL 5947735, at *2 (D. Mass. Aug. 31, 2020).
148. U.S. CHAMBER OF COMMERCE, BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY 1 (2014).
149. *Id.* at 3.
150. *Id.*
151. *Id.*
152. *Id.* at 5.
153. *Id.* at 2.

increase because more individuals are working, products are being bought, and thus economies develop.[154]

The European Centre for International Political Economy also illustrates the extensive penetration of data and the need for cross-border data transfers in their report titled: *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce.*[155] In offering an illustration of data movement and the inevitable chain of data transfers, the report states that before a purchase can be made in a store, "a number of different services, such as utilities, consulting, engineering… were [probably] needed to produce the good."[156] After producing such goods, the vendor of the good "needs leasing, distribution, logistics and facility management services to deliver the good."[157] Finally, as goods and data are transferred to the store selling the item, "a purchase made in a store requires access to card processing and other financial services backed by data transmission… to process the transaction."[158] Data is created as businesses meet demand and attempt to increase revenue.[159] As such, all business interactions and transactions require a transfer of a combination of employee, consumer, and corporate data to conduct everyday business functions.[160]

Understanding the importance of international data transfers, Chapter 5 of the GDPR establishes guidelines for individuals and corporations concerning the transfer of personal data overseas.[161] Transferring data under the GDPR may only take place under one of two conditions.[162] First, if a country's data privacy regime adequately meets the standards set out by the GDPR and qualifies for an adequacy decision, any corporation linked to that country may transfer data freely between the EU and such country.[163] The second condition is more complex in that if the country does not qualify for an adequacy decision, the country or corporation needs to provide appropriate safeguards subject to EU standards to transfer data offshore.[164] Because the U.S. law relies on a mix of legislation, regulation, and self-regulation by corporations, the European Commission ("EC"), which grants adequacy decisions, deems American data privacy law to be inadequate to safeguard European data subject's interests and thus has not allowed for the free transfer of data to the United States.[165] This has caused a serious burden for businesses as the lack of a federal standard means that businesses have to establish facilities and safeguards in Europe, spend substantial time and money to become GDPR compliant through other means, or forfeit collecting, processing, and transferring any European data within or to the United States.[166] To circumvent this cross-border transfer issue regarding adequacy of data privacy laws and enable U.S. companies to

154. *Id.* at 4.
155. U.S. CHAMBER OF COMMERCE, THE ECONOMIC IMPORTANCE OF GETTING DATA PROTECTION RIGHT: PROTECTING PRIVACY, TRANSMITTING DATA, MOVING COMMERCE (2013).
156. *Id.* at 5.
157. *Id.*
158. *Id.*
159. U.S. CHAMBER OF COMMERCE, *supra* note 148, at 1.
160. *Id.*
161. GDPR, *supra* note 118, at 60–65.
162. *Id.* at art. 45-46, 2016 O.J. (L 119) 61-62.
163. *Id.* at art. 45 2016 O.J. (L 119) 61.
164. *Id.* at art. 46, 2016 O.J. (L 119) 62.
165. *Overview*, INT'L TRADE ADMIN., https://www.privacyshield.gov/article?id=OVERVIEW (last visited Sept. 26, 2022).
166. *Id.*

transfer data freely between the two regions, the EU and U.S. created the EU-U.S. Privacy Shield Framework in 2016.[167]

The Privacy Shield was designed to provide companies in the U.S. and Europe with a mechanism to comply with data protection requirements within the GDPR and enable corporations to transfer personal data from the European Union to the United States.[168] While the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable corporations to transfer data offshore under EU law, in 2020, the Court of Justice of the EU issued a judgment declaring the Commission's decision invalid.[169]

The Data Protection Commissioner v. Facebook Ireland Ltd., Maximillian Schrems (C-311/18), also known as *Schrems* II, expresses the EU Court of Justice's decision to invalidate the EU-U.S. Privacy Shield Framework.[170] Even before *Schrems* II and the EU-U.S. Privacy Shield, the concept of the unrestrained movement of data overseas was targeted by consumer rights activists in Europe.[171] In particular, in *Schrems* I, Max Schrems brought suit against the Irish Data Protection Commission ("DPC") and Facebook Ireland because the Irish DPC refused to suspend data transfers from Facebook Ireland to Facebook in the U.S. in 2013.[172] Max Schrems's concern was rooted in Edward Snowden's "whistleblowing" revelations concerning U.S. surveillance practices, and Schrems complained that Facebook violated his EU data protection rights because his personal data could be accessed by U.S. intelligence authorities.[173] As a result of *Schrems* I in 2013, the Safe Harbor mechanism—the predecessor to the EU-US Privacy Shield—was invalidated and the free flow of data transfers to the U.S. was halted.[174]

After the 2013 decision, the U.S. and EU created the Privacy Shield to reestablish a method that would minimally burden overseas data transfers for U.S. corporations.[175] As the U.S. and EU fixed the data transfer mechanism by implementing the Privacy Shield, Max Schrems brought a similar claim against the Irish DPC on the basis that Facebook's European headquarters in Ireland continued transferring personal data from its European headquarters in Ireland to the US and violated his EU data protection rights.[176] On July 16, 2020, the Court of Justice of the European Union declared the EU-U.S. Privacy Shield invalid.[177] The court reasoned that U.S. laws do not satisfy requirements essential to EU law because of inadequate data privacy laws.[178] The court stated that U.S. law provides limited protection for data

167. *Privacy Shield Program Overview*, INT'L TRADE ADMIN., https://www.privacyshield.gov/program-overview (last visited Sept. 26, 2022).
168. *Id.*
169. INT'L TRADE ADMIN., *supra* note 167; Council Directive 2016/1250 of July 12, 2016, The European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 2017) 6,16 [hereinafter Adequacy of EU-U.S. Privacy Shield];
Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (Schrems II), ECLI:EU:C:2020:559, ¶¶ 42–49 (July 16, 2020).
170. Adequacy of EU-U.S. Privacy Shield, *supra* note 169; *Schrems II*, at ¶¶ 42–49.
171. *Max* Schrems, IAPP, https://iapp.org/resources/article/max-schrems (last visited Sept. 26, 2022).
172. *Schrems I*, IAPP, https://iapp.org/resources/article/schrems-i (last visited Sept. 26, 2022).
173. *Id.*
174. *The Definitive Guide to Schrems II*, DATAGUIDANCE, https://www.dataguidance.com/resource/definitive-guide-schrems-ii (last updated Mar. 25, 2022).
175. *Id.*
176. *Id*.
177. *Id.*
178. *Id.*

subjects because U.S. laws enable U.S. public authorities to freely access and use data related to EU data subjects.[179] The court also invalidated the EU-U.S. Privacy Shield because U.S. data privacy law would not provide a substantial equivalent cause of action for data subjects as required by EU law if an EU data subject's data privacy rights were infringed on.[180]

Schrems II affects global trade and business.[181] In particular, U.S. businesses that were originally protected by the Privacy Shield cannot use the Shield as a framework to transfer data from the EU to the U.S. and must use alternative transfer mechanisms such as standard contractual clauses to transfer data.[182] While large corporations can easily handle drafting standard contractual clauses related to consumer consent and data privacy, the *Schrems* decisions plague small and medium-sized businesses because many lack legal departments to implement data protection clauses.[183] The Privacy Shield was crucial for small and medium-sized businesses as it established a legal mechanism for smaller businesses to self-certify their data protection systems and transfer data to the U.S. from the EU, but *Schrems II* invalidated this mechanism.[184] The invalidation also created substantial burdens on U.S. businesses as entities needed to incur additional costs, and navigate various risks and complexities in trying to transfer data out of Europe.[185] Finally, this change has caused all businesses to decide whether to continue transferring data from the EU or simply withdraw from transatlantic trade.[186] As a result of this change, many businesses have temporarily closed shop in the EU or left the European market completely.[187]

The economic effect of *Schrems* II is further felt through statements made by the Biden Administration in 2022.[188] The free flow of data between the U.S. and Europe underpins "more than $1 trillion in cross-border commerce."[189] Based on such numbers, the U.S. and European companies lost more than $2 trillion worth of commerce due to the lack of a comprehensive data privacy framework within the United States.

Cross-border data transfer issues also plague U.S. companies outside the GDPR and EU. South Korea, for example, adopts a similar data privacy standard to the

179. *Id.*
180. *Id.*
181. *The Results Are In: How Schrems II Will Impact International Data Flows in Practice*, FIELDFISHER (Sept. 9, 2020), https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/how-schrems-ii-will-impact-international-data-flow.
182. Nigel Cory et al., *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, ITIF (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic.
183. *Id.*
184. *Id*.
185. *Id.*
186. *Id.*
187. *Closing Shop or Closing Off: Companies Respond to GDPR*, TREND MICRO INC. (May 31, 2018), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/closing-shop-or-closing-off-companies-respond-to-gdpr.
188. *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, THE WHITE HOUSE (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework.
189. *Id.*

GDPR through its Personal Information Protection Act ("PIPA").[190] While the U.S.-Korea Free Trade Agreement (KORUS) explicitly states that U.S. companies should be allowed to freely transfer the personal data of clients from South Korea to the United States,[191] PIPA limits the transferability of personal data overseas and makes "free" cross-border transfers difficult.[192] Consequently, U.S. companies have difficulties transferring data to the U.S. and are forced to spend funds to establish data hubs within South Korea and to abide by South Korean standards.[193] If the U.S. had a GDPR-like standard or an adequacy decision from the EC stating that U.S. data privacy laws were adequate, however, cross-border transfers would be substantially easier for U.S. companies.

Another example is Argentina's Data Protection Act ("PDPA"): the PDPA prohibits corporations and other organizations from transferring personal data to countries that do not have adequate levels of protection in place.[194] If the U.S. was deemed to be a country with inadequate personal data laws, corporations would need to decide whether to stay in the Argentine market without the ability to transfer data to the U.S. or to withdraw from the market completely.[195]

The ability to collect, process, and transfer data freely overseas are crucial to business growth, technological development, and the global economy.[196] The GDPR sets a standard that protects consumer data privacy rights while ensuring that businesses can transfer data safely.[197] However, due to the lack of regulation within the U.S., companies are unable to conduct business efficiently and are driven to expend substantial funds in order to comply with laws around the world.[198] If the U.S. were to adopt a comprehensive law at the federal level similar to the GDPR, U.S. companies would be less burdened in accessing global markets and be able to grow revenue while protecting consumers in the U.S. and globally.[199]

VI. INTERNATIONAL SOLUTIONS

While the GDPR and data protection laws in other countries restrict U.S. companies, other countries have solved cross-border data transfer issues by amending

190. Geinjeongbo Bohobeop [Personal Information Protection Act] (S. Kor.).
191. The United States – Korea Free Trade Agreement, June 30, 2007.
192. Personal Information Protection Act, art. 39-12 (S. Kor.).
193. *Beopryeonghaeseok: Gaeinjeongbocheorireul Gukoe Je3jaege Witaksi Jeongbochujeui Dongui Piryo Yeobu* [*Law Interpretation: Whether or Not Consent is Required when Entrusting the Processing of Personal Information to an Overseas Third Party*] reply 210429 GEUMYUNGGYUJE · BEOPRYEONGHAESEOKPOTEOL [FIN. REG. AND L. INTERPRETATION PORTAL] Dec. 16, 2021 (S. Kor.).
194. Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost*, ITIF (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost; Law No. 25.326, Oct. 30, 2000 (Arg.).
195. Matt Davis, *The EU-US Privacy Shield Invalidated: What This Means For You*, OSANO (July 29, 2020), https://www.osano.com/articles/privacy-shield-invalidated; Ashley Thomas, *Privacy Shield Invalidated: Implications for US Businesses*, LAW. MONTHLY (Dec. 2, 2020), https://www.lawyer-monthly.com/2020/12/privacy-shield-invalidated-implications-for-us-businesses.
196. Tanguay van Overstraeten, *Cross-Border Data Flows: A Necessary Part of Global Trade*, AMCHAM EU (June 11, 2021), https://www.amchameu.eu/blog/cross-border-data-flows-necessary-part-global-trade.
197. *See generally* GDPR, *supra* note 118.
198. Luke Irwin, *How Much Does GDPR Compliance Cost in 2022*, IT GOVERNANCE (Apr. 26, 2022), https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020.
199. Tim Woods, *Three Ways GDPR Benefits US Companies*, HELP NEW SEC. (May 10, 2019), https://www.helpnetsecurity.com/2019/05/10/gdpr-benefits-us-companies.

or adopting data privacy laws to be similar to the GDPR and obtaining adequacy decisions from the EC.[200] South Korea, for example, established PIPA in 2011 which preceded the inception of the GDPR in 2018.[201] In its original form, PIPA organized data privacy standards within South Korea by setting up an individual enforcement committee to protect data subject rights,[202] outlining specific rights for businesses to collect and process information,[203] and implementing restrictions related to cross-border transfers of data.[204] At its inception, the concept of unrestricted data transfers overseas was not implemented and cross-border transfers were subject to the explicit consent of data subjects.[205] By 2015, however, foreign businesses in South Korea struggled with Korean data localization and the EU and Korea executed a Free-Trade Agreement that enabled unrestrained cross-border data transfers as long as the data privacy laws of each signing country acted similarly to the opposite party's laws.[206] After this, the EU created the GDPR in 2018 and South Korea strengthened its data privacy laws by amending PIPA with GDPR-like concepts.[207] Subsequently, the European Commission decided that South Korea offers adequate protection of personal data and thus businesses incorporated in South Korea can easily transfer data from the EU to South Korea[208] and do not have to worry about additional expenditures on data privacy, losing out on international markets, and being subjected to extreme litigatory costs in Europe.[209]

Japan is another country that amended its data privacy laws to receive preferential treatment from the EC and maintains the privilege to transfer data freely across borders. In amending its Act on the Protection of Personal Information ("APPI") in 2017, Japan strengthened its data processing laws to subject companies located outside of Japan to stricter guidelines.[210] By adopting stricter guidelines, Japan and the EC reached an agreement on the "reciprocal adequacy" of their respective data protection laws meaning that Japanese data protection laws are similar to the GDPR.[211] As a result, Japanese and European companies may process, collect

200. Simmons, *supra* note 144; *Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 10, 2022).
201. *Compare* Geinjeongbo Bohobeop *supra* note 190, *with* GDPR, *supra* note 118, at 1.
202. Geinjeongbo Bohobeop [Personal Information Protection Act] art. 7 (S. Kor.) (2011).
203. *Id.* art. 15.
204. *Id.* at art. 17.
205. *Id.* at art. 17(3).
206. Council Directive 2011/265 of Sept. 16, 2010, Free Trade Agreement Between the European Union and Its Member States, 2011 O.J. (L 127).
207. Geinjeongbo Bohobeop [Personal Information Protection Act] (S. Kor.) (2020).
208. Commission Regulation 2022/254 of Dec. 17, 2021, Adequate Protection of Personal Data by the Republic of Korea Under the Personal Information Protection Act, 2021 O.J. (L 44) 1.
209. *See generally EU Adopts 'Adequacy' Decisions Allowing Data to Continue Flowing Freely to the UK*, DEP'T FOR DIGIT., CULTURE, MEDIA & SPORT (June 28, 2021), https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk (highlighting the benefits that the United Kingdom would experience because of extension of an adequacy decision. Because South Korea was granted an adequacy decision, like the United Kingdom, the benefits will likely be similar).
210. Hiroyuki Tanaka & Noboru Kitayama, *Japan Enacts Amendments to the Act on the Protection of Personal Information*, IAPP (June 9, 2020), https://iapp.org/news/a/japan-enacts-the-act-on-the-protection-of-personal-information.
211. KOJIN' JŌHŌNO HOGONI KAN'SURU HŌ [ACT ON THE PROTECTION OF PERSONAL INFORMATION] (Japan); European Commission Press Release IP/19/421, The Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019).

and transfer data freely across their borders as both the EU and Japan recognize that their laws allow personal data to be transferred safely overseas.[212]

In adopting new legislation, New Zealand adopted a set of privacy rules that followed GDPR standards in implementing the Privacy Act 2020 ("2020 Act").[213] The Privacy Act reformed procedures taken by businesses when data breaches occur, adjusted fines imposed due to non-compliance, and mandated that all New Zealand businesses take reasonable steps to confirm that jurisdictions, where data was being sent, had appropriate privacy laws or that the businesses and clients had contractual obligations that would protect the data subject's sensitive data.[214] In order to reflect GDPR standards and easily obtain adequacy from the EC, New Zealand added requirements regarding cloud storage and security, mandatory data breach notifications, and an extraterritorial effect subjecting overseas businesses that operate in New Zealand to Privacy Act privacy obligations.[215]

Countries around the world have solved the cross-border data transfer problem by modifying existing laws or creating new laws to reflect similar standards to the GDPR. Due to such acts, the European Commission has recognized other countries like Argentina, Canada, and Switzerland for adequacy decisions stating that these counties provide adequate data protection laws and thus, entities in these counties are able to collect, process and transfer data freely across their borders.[216]

VII. DOMESTIC EFFORTS: ALMOST THERE, BUT NOT GOOD ENOUGH

As outlined in Part II of this article, because the U.S. has yet to adopt a comprehensive data privacy framework, the government has tried resolving data privacy issues through a patchwork of sector-specific federal laws, leaving other data privacy issues up to state legislatures to resolve, and relying on judicial decisions to pick up scraps.[217]

Sector-specific federal laws set a complex framework for data privacy laws within the United States.[218] In addition to 15 U.S.C. § 45 charging the FTC with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce," the FTC relies on various acts like the Privacy Act of 1974 and Fair Credit Reporting Act to enforce privacy promises.[219] However, these acts fall short of GDPR standards because they only extend to the federal government, and provide broad loopholes which businesses can easily maneuver around to transfer information with ease.[220]

The issue with relying on sector-specific federal data privacy laws is that such laws either spill over to other industries and overburden businesses and data

212. *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows*, EUR. COMM'N (Jan. 23, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.
213. *The Privacy Act 2020 & GDPR Adoption in New Zealand*, RUNECAST (Nov. 30, 2020), https://blog.runecast.com/blog/h1-4-60-characters-the-privacy-act-2020-gdpr-adoption-in-new-zealand.
214. *Id.*
215. *Id.*
216. EUROPEAN COMM'N, *supra* note 200.
217. Klosowski, *supra* note 21.
218. *Id.*
219. *Id.*
220. *See* discussion *supra* Part II.

subjects or fail to close gaps related to protecting personal data thus creating further complexity, inconsistency, and uncertainty for businesses.[221] Because U.S. statutes regulate based on the type of personal data and the type of organization accessing and holding such data, only a fraction of an individual's personal data is regulated when the data is maintained by a certain type of entity.[222] For example, HIPAA creates a standard to protect sensitive patient health information from being disclosed without a patient's consent.[223] However, HIPAA does not protect all health data, but only applies to data used for health plans, health care providers who conduct certain financial and administrative transactions, health clearinghouses, and business associates.[224] Therefore, health data held by a company or person, who is not considered a covered entity or business associate under HIPAA, is not required to comply with outlined data privacy standards.[225] This demonstrates that HIPAA does not protect patient health data that is used by companies that do direct-to-consumer genetic testing, or mobile apps, like fitness-tracking apps, that require users to enter their own health information.[226] Because HIPAA only covers certain entities and types of data, data privacy laws fall short in terms of completely protecting a data subject's sensitive health information in all aspects of life and business.

The FCRA is also a perfect example of the contradictory nature of U.S. data privacy law.[227] In attempting to establish data privacy rights for consumers, the FCRA protects consumers by regulating how certain data collectors disseminate and use client credit information.[228] The FRCA extends expansive coverage over such data by granting jurisdiction over "any person which, for. . . fees, [or] dues regularly engages in whole or part in practice of assembling. . . consumer credit information. . . for the purpose of furnishing consumer reports to third parties."[229] Accordingly, the FCRA data privacy requirements apply to all companies that conduct background checks on job applicants[230] and market financial products.[231] As mentioned in Part II, while a company can obtain consumer reports as long as they have a "legitimate business need," such companies are subject to data privacy provisions within the FCRA.[232] The FCRA encompasses many businesses and can extend to essentially any corporation, partnership, or individual doing commerce and using credit information which places a large burden on individuals as they attempt to comply with the FCRA.[233]

221. Klosowski, *supra* note 21.
222. *Id.*
223. 42 U.S.C. § 1320d-2.
224. 45 C.F.R. § 160.102 (2022).
225. Solove, *supra* note 78.
226. *Medical and Health Data Privacy: HIPAA and Beyond: Health Data Not Covered by HIPAA*, FRANKLIN CNTY. L. LIBR., https://fclawlib.libguides.com/HIPAA/notHIPPAA (last updated Oct. 13, 2022).
227. *See e.g.,* 15 U.S.C. § 1681.
228. *A Summary of Your Rights Under the Fair Credit Reporting Act*, CONSUMER FIN. PROT. BUREAU, https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf (last visited Sept. 26, 2022).
229. 15 U.S.C. § 1681a(f).
230. Hyongsoon Kim et. al, *Critical Considerations for Compliance with the FCRA*, AKIN GUMP (June 18, 2019), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/critical-considerations-for-compliance-with-the-fcra.html.
231. https://files.consumerfinance.gov/f/documents/102012_cfpb_fair-credit-reporting-act-fcra_procedures.pdf
232. Jacquez & Friend, *supra* note 82.
233. *Id.*

On the other hand, the FCRA lacks requirements related to notifications to consumers regarding data breaches, procedures to ensure that data remains in the correct hands after transfers to third parties, and methods that guarantee that third parties accessing sensitive credit information are using it appropriately.[234] The lack of certain requirements enables companies to share sensitive information with third parties who can later sell data to other individuals without notifying the original data subject.[235] From a consumer perspective, these gaps an individual's ability to trust and use a business's system.[236] However, because there is no other law that protects such information or the transfer of data, consumers are left to put blind trust in corporations and hope that their sensitive data remains protected.[237] As a result, the EU and other countries do not trust American data privacy law because it fails to safeguard data.[238]

With lacking federal law, states have approached data privacy through state legislation.[239] States that currently have comprehensive data privacy laws are California, Virginia, Utah, Colorado, and Connecticut.[240] While these states have adopted similar provisions regarding the type of notice and the choice of a data subject controlling their own data, most of these state laws fall short of GDPR standards.[241] Moreover, the furthering of data privacy patchwork through state privacy laws only serves to create more confusion as state laws do not provide for interstate commerce and data transfer regulations.[242] State laws also raise the costs of doing business and complicate compliance as each business operation in various states will have to comply with different rules which will create an inefficient marketplace.[243] As a result, relying on state legislatures to adopt data privacy laws is not a viable solution.

To complicate matters even further, because most federal and state laws lack provisions regarding safeguards on data when transferred from one entity to another, the U.S. judiciary has stepped in to fill the void.[244] In doing so, U.S. courts have essentially guaranteed the right for corporations to transfer data freely without substantial checks and protections on data by referencing the First Amendment of the U.S. Constitution.[245] In expanding business's rights to use and transfer data freely, the Supreme Court analyzed the data rights of pharmaceutical research companies and manufacturers in *Sorrell v. IMS Health Inc*.[246] In its decision, the Supreme Court held that a Vermont state statute violated the First Amendment rights

234. *Id.*
235. Klosowski, *supra* note 21.
236. *Id.*
237. *Id.*
238. Hendrik Mildebrath, *The CJEU Judgement in the Schrems II Case*, EUR. PARLIAMENTARY RSCH. SERV. (Sept. 2020), https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.
239. Klosowski, *supra* note 21.
240. *Id.*
241. *Id.*
242. *The Argument for a National US Data Privacy Framework*, OPEN ACCESS GOV'T (Sept. 29, 2021), https://www.openaccessgovernment.org/us-data-privacy-framework/121292.
243. *Id.*
244. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 576–80 (2011). *See also* Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018); Lloyd v. Google LLC. [2021] UKSC 50 (appeal taken from Eng.).
245. See *Sorrell*, 564 U.S. at 557; *Carpenter*, 138 S. Ct. at 2214–15; Lloyd v. Google LLC. [2021] UKSC 50 (appeal taken from Eng.).
246. *Sorrell*, 564 U.S. at 561–563.

of various health-related companies because it banned the sale, transmission, and use of personal health information. In doing so, the Court reasoned that the "creation and dissemination of information" are within the meaning of the First Amendment, and because of this rule, the prescriber-identifiable information transmitted and used was considered speech.[247] The Court also added that the information was protected by the First Amendment because it could readily identify data subjects and by placing a ban on its use, the Vermont statute would put a content- and speaker-based burden on the speech.[248] Thus, the Court held that corporations could freely use and transfer sensitive information and have vastly expanded business authorities to transfer information domestically.[249]

The approach taken in *Sorrell* is problematic because many have interpreted its holding as a conclusion to "whether a flat restriction on data disclosure constitutes an abridgment of free speech."[250] The legal analysis provided by *Sorrell* does not limit itself to restrictions on prescriber-identifying information, but it governs all information disclosures.[251] Accordingly, *Sorrell*'s decision could possibly extend its reach to all sales and disclosures of any information, such as personal medical information, purchase history, and personally identifiable information.[252] Under this approach, minimal protection is offered to individuals if they hope to protect their data and wish to know where it is transferred. Thus, in comparison with the GDPR and standards that are desired by other countries, cross-border transfers between operations in other countries may be difficult because *Sorrell* invalidates any restriction on data that is held by businesses and enables businesses to use data to the greatest extent possible.[253]

With the chaos created by the mixture of federal and state laws along with judicial decisions within the U.S., corporations have ultimately set aside U.S. standards and resorted to equipping themselves with the tools and compliance methods necessary to adhere to GDPR standards.[254] U.S. companies comply with these standards because compliance with the GDPR is mandatory to do business within the EU and because penalties for non-compliance are significant.[255] In addition, jurisdictional issues would arise as corporations offer goods and services to individuals in the EU or monitor the behavior of certain individuals to better promote their products.[256] As a requirement of the GDPR, most foreign companies that are subject to the GDPR must have a representative located within the European Union as well.[257] As a result, most multinational companies have resolved to simply follow GDPR standards throughout their entity regardless of where the business is located

247. *Id.* at 570, 580.
248. *Id.* at 564.
249. Bastian Shah, Note, *Commercial Free Speech Constraints on Data Privacy Statutes After Sorrell v. Ims Health*, 54 COLUM. J.L. & SOC. PROBS. 93, 128 (2020).
250. Ashutosh Bhagwat, *Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 855 (2012).
251. *Id.* at 868.
252. *Id.*
253. *Id.* at 870.
254. *GDPR for US Companies*, COMPLIANCE JUNCTION, https://www.compliancejunction.com/gdpr-for-us-companies (last visited Nov. 23, 2022).
255. *Id.*
256. *Key Compliance Issues for US Companies*, STEPTOE, https://www.steptoe.com/images/content/1/4/v3/140575/GDPR-ComplianceChecklist.pdf (last visited Sept. 26, 2022).
257. *Id.*

in order to incur fewer costs and not deal with the complexity and confusion associated with U.S. data privacy law.[258]

VIII. PENDING U.S. RESPONSES: HISTORY WILL REPEAT ITSELF

At present, the U.S. government has responded to international and domestic data privacy matters in two ways. First, the U.S. has engaged the European Union in order to implement another bilateral data privacy framework.[259] Second, members of Congress have introduced various data privacy-related bills that look to establish a national framework for data privacy.[260]

On March 25, 2022, the U.S. government and European Commission announced an "agreement in principle" to create a new data privacy framework to enable U.S. companies to transfer personal data across borders.[261] The pending arrangement will replace the Privacy Shield that was invalidated by the Court of Justice of the European Union ("CJEU") through its holding in Schrems II.[262] Despite efforts to create a new data privacy framework, many speculate that the pending framework sets the table for a potential "Schrems III."[263] Considering that the CJEU has invalidated EU-U.S. data privacy frameworks twice before because of the lack of protection related to the rights of data subjects, it is likely that there will be another challenge that could further burden U.S. individuals and businesses.[264] Clearly, recreating a similar framework is not a viable solution that will enable businesses to freely transfer data, and if challenged, U.S. and European businesses will potentially lose more than one trillion dollars again in cross-border commerce due to a failure to transfer data.[265]

Moreover, the pending agreement would not solve the global issue of U.S. companies being heavily restricted from transferring data from other countries to the United States.[266] Even though the framework would demonstrate to the world that the EU seeks to do business with the U.S. and allows for cross-border data transfers, the agreement would only extend to members of the European Union.[267] As long as the U.S. does not have a similar federal law to the GDPR, these countries will continue to heavily restrict U.S. companies and their control of data, regardless

258. *Id.*
259. THE WHITE HOUSE, *supra* note 188.
260. Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker (last updated Aug. 2, 2021).
261. Rajesh De et. al, *US and EU Announce New Trans-Atlantic Data Privacy Framework*, MAYER BROWN (Mar. 29, 2022), https://www.mayerbrown.com/en/perspectives-events/publications/2022/03/us-and-eu-announce-new-transatlantic-data-privacy-framework.
262. *Id.*
263. Simon McMenemy et. al, *The U.S. and EU Announce an "Agreement in Principle" to Replace the EU-U.S. Privacy Shield Framework: What Employers Need to Know*, NAT. L. REV. (Mar. 31, 2022), https://www.natlawreview.com/article/us-and-eu-announce-agreement-principle-to-replace-eu-us-privacy-shield-framework; Malcolm Dowden & Rosa Barcelo, *United States and European Commission Announce Trans-Atlantic Data Privacy Framework: Setting the Scene for Schrems III?*, NAT. L. REV. (Mar. 28, 2022) https://www.natlawreview.com/article/united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework.
264. *Id.*
265. THE WHITE HOUSE, *supra* note 188
266. Elizabeth Harding et. al, *Data Localization and Data Transfer Restrictions*, NAT. L. REV. (Aug. 10, 2021), https://www.natlawreview.com/article/data-localization-and-data-transfer-restrictions.
267. *See* sources cited *supra* note 170 and accompanying text.

of the framework created between the EU and U.S., as they had done even when the EU-U.S. Privacy Shield was valid.[268]

A second way that the U.S. has attempted to address its deficiency in data privacy law has been to introduce bills during Congressional sessions aimed at resolving data privacy issues. Representative Suzan DelBene, for example, has made efforts to establish a national framework for data privacy by introducing the Information Transparency and Personal Data Control Act.[269] The bill (H.R. 6864) was first introduced to the U.S. House of Representatives during the 115th Congressional session in 2018.[270] The bill sought to require the FTC to "promulgate regulations related to sensitive personal information or behavioral data."[271] These regulations would apply to "any operator that provides services to the public involving the collection, storage, processing, sale, sharing with third parties, or other use of sensitive personal information for United States persons or persons located in the United States."[272] The regulation would also require such data controllers to meet standards regarding affirmative, express, and opt-in consent from data users, a corporation's privacy and data use policy, opt-out options for clients, and privacy audits.[273] Notwithstanding, the bill was referred to the House Committee on Energy and Commerce and failed to emerge from committee hearings.[274]

Since 2018, Representative Delbene has reintroduced the Information Transparency & Personal Data Control Act to the House of Representatives in the 116th and 117th sessions of Congress.[275] In its most recent form, H.R. 1816 looks to broaden individuals' rights to control their personal data by requiring the FTC to create regulations related to opt-in and opt-out options, a corporation's privacy and data use policy and privacy audits.[276] The act also seeks to establish a uniform set of rules for businesses to operate in and provide a clear domestic policy related to data privacy.[277]

However, many predict the bill to fail during this session like its counterparts in former sessions.[278] A major flaw with the current bill is the lack of a provision regarding an individual's right to action.[279] While H.R. 1816 provides that the FTC and state attorney generals may bring an action, an individual does not have a right to bring an action against a data controller that misuses her information.[280] The GDPR, for example, provides a private right of action to data subjects and enables them to pursue litigation to ensure that their privacy rights are not infringed upon

268. Harding, *supra* note 266.
269. Information Transparency & Personal Data Control Act, H.R. 6864, 115th Cong. (2018).
270. *Id.*
271. *Id.*
272. *Id.* § 2(a).
273. *Id.*
274. *HR 6864 (115th): Information Transparency & Personal Data Control Act*, GOVTRACK, https://www.govtrack.us/congress/bills/115/hr6864 (last visited Nov. 23, 2022).
275. *See* Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019). *See also* Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. (2021).
276. H.R. 1816, 117th Cong. §§ 2(6), 3(a) (2021).
277. Daniel Friedman, *Information Transparency and Personal Data Control Act Introduced in Congress*, NAT. L. REV. (Apr. 2, 2021), https://www.natlawreview.com/article/information-transparency-and-personal-data-control-act-introduced-congress.
278. *H.R. 1816: Information Transparency & Personal Data Act*, GOVTRACK, https://www.govtrack.us/congress/bills/117/hr1816 (last visited Nov. 23, 2022).
279. Friedman, *supra* note 277.
280. *Id.*

by corporations.[281] Not only does the GDPR provide a mechanism for a private right of action under Article 82(1), but also Article 80(2) enables an individual to mandate a "not-for-profit" institution to assist with bringing suit.[282] The right to file suit also includes the ability to bring class action lawsuits.[283] H.R. 1816, however, does not provide these rights to data subjects thus lacking a crucial element related to data privacy.[284]

Opposition against H.R. 1816 also arises as businesses complain that complying with data privacy laws is expensive, time-consuming, and difficult.[285] H.R. 1816 does not provide incentives for businesses or financial assistance to small businesses and startup companies that have limited revenue to allocate to data compliance and privacy maintenance.[286] Thus, H.R. 1816 is expected to fail due to limited support by individuals and businesses, and the U.S. will go to another Congressional session without establishing a comprehensive federal data privacy law.

IX. PROPOSED SOLUTION

As noted, current domestic solutions fall short of the international threshold needed to receive favorable treatment from data-privacy-stringent countries.[287] U.S. data privacy laws are complex, convoluted, and confusing because of the United States' sector-specific approach, weak federal framework, and varying state laws.[288] In spite of its current attempt to enact a comprehensive data privacy law, H.R. 1816 is inadequate in its current form to provide individuals substantial data protection, promote U.S. companies to establish appropriate data protection measures, and gain favor with the European Commission as well as the world.

My proposed solution is not only to establish a federal law on data protection and privacy by amending H.R. 1816 to reflect certain aspects of the GDPR, but also to amend H.R. 1816 in a way that businesses, regardless of size, do not incur significant costs in adhering to more defined data privacy regulations. This solution would allow U.S. individuals and companies to transfer data to and from other countries and develop more efficient business practices as well.

To offer more significant protection for individual data privacy rights, H.R. 1816 should be revised to reflect GDPR standards. Like the GDPR, H.R. 1816 should include provisions related to companies providing data subjects with personalized notices regarding the use of their information, data breach disclosures, and a right for individuals to file an action against companies that misuse a data subject's information.[289]

---

281. *GDPR Provides a Private Right of Action. Here's Why That's Important.*, X1 DISCOVERY INC., https://www.x1.com/2018/02/28/gdpr-provides-a-private-right-of-action-heres-why-thats-important (last visited Sept. 26, 2022).
282. *Id.*
283. *Id.*
284. GOVTRACK, *supra* note 278.
285. Daniel Mikkelsen et. al, *GDPR Compliance Since May 2018: A Continuing Challenge*, MCKINSEY & CO. (July 22, 2019), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge.
286. H.R. 1816, 117th Cong. §§ 2(6), 3(a) (2021).
287. COMM'N, *supra* note 200.
288. Klosowski, *supra* note 21.
289. Herny H. Eckerson, *GDPR Reference Guide: All 99 Articles in 25 Minutes*, ECKERSON GRP. (Nov. 28, 2017), https://www.eckerson.com/articles/gdpr-reference-guide-all-99-articles-in-25-minutes.

Personalized notices related to the use of a data subject's information are essential to protecting consumers while building trust in business entities.[290] While H.R. 1816 mandates that companies provide public policies that use plain language for consumers to understand,[291] such policies are typically overlooked and many people do not know how their data is being used or where it is being transferred.[292] The FTC has stated, in general, "privacy policies do a poor job of informing consumers about companies' data practices or disclosing changes to their practices."[293] The GDPR and other global data privacy laws require that business entities provide personalized notice to data subjects regarding the exact use of their data, the recipients of such information, and how an entity intends to use a client's data in cross-border transfers.[294] As businesses ensure that individuals are informed about the location and use of their data, data subjects can better trust companies to not misuse information. A personalized notice regarding one's data would also protect companies from litigation as they take an individualized approach and discuss specifics related to the broad uses of an individual's data.

Data breach disclosures greatly benefit individuals, as well as shareholders and companies.[295] Mandatory disclosures foster communication with data subjects and enhance trust in a company's brand and image.[296] By requiring businesses to communicate data breaches to individuals, data subjects can quickly respond by taking measures to ensure that information stored elsewhere does not become compromised.[297] Furthermore, a national standard benefits individuals and shareholders because it would encourage managers and directors of corporations to take constant action to reduce risk and a firm's exposure to breaches.[298]

Notwithstanding these other recommendations, the most pivotal aspect that must be added to any federally comprehensive bill about data privacy is an individual's right of action against a breaching data controller.[299] In its current form, H.R. 1816 does not provide a private right of action.[300] A private right of action protects individuals as it allows data subjects that are harmed by a violation of their privacy rights to hold perpetrators accountable and obtain necessary redress.[301] Moreover,

290. Timothy Morey et. al, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.
291. H.R. 1816, 117th Cong. § 3(a)(2)(A) (2021).
292. Morey et al., *supra* note 290.
293. Patrick Fowler, *Why You Need a Privacy Policy – Part 2: Avoiding Three Common Fumbles*, SNELL & WILMER (Mar. 13, 2015), https://www.jdsupra.com/legalnews/why-you-need-a-privacy-policy-part-2-64809.
294. GDPR, *supra* note 118, at art. 13(1), 2016 O.J. (L 119) 40-41.
295. Steve Klemash, Jamie Smith, & Check Seets, *What Companies are Disclosing About Cybersecurity Risk and Oversight*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 25, 2020), https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.
296. Juliette Rizkallah, *When A Data Breach Can Be A Benefit To Your Brand*, FORBES (July 11, 2017, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/07/11/when-a-data-breach-can-be-a-benefit-to-your-brand/?sh=47e8ea8f4e6e.
297. *Id.*
298. Musaib Ashraf & Jayanthi Sunder, *Can Shareholders Benefit From Consumer Protection Disclosure Mandates? Evidence From Data Breach Disclosure Laws*, ACCT REV. (forthcoming 2023).
299. *A Private Right of Action is Key to Ensuring that Consumers Have Their Own Avenue for Redress*, NEW AM., https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress (last visited Apr. 28, 2022).
300. *See generally* H.R. 1816, 117th Cong. (2021).
301. Paula Bruening, *How to End the Deadlock on the Private Right of Action*, IAPP (Jan. 20, 2022), https://iapp.org/news/a/how-to-end-the-deadlock-on-the-private-right-of-action.

a private right of action would relieve government agencies like the FTC from having to pursue actions and would allow individuals who are truly harmed to seek direct relief.[302] An individual cannot truly be protected unless they are able to pursue solutions and obtain redress. A government agency pursuing action would only harm a company while not addressing the core issue of affording redress for a data subject whose information has been misused, tampered with, or stolen. However, if an individual were able to bring a claim against a company under a private right of action, class action lawsuits would likely emerge, and businesses would be more likely to take steps to ensure that data is adequately protected.

One of many criticisms of a uniform data privacy law is that it would impose significant costs on U.S. businesses and the economy.[303] According to the Information Technology and Innovation Foundation ("ITIF"), if Congress were to pass legislation that significantly copied the GDPR, it would cost the U.S. economy $122 billion annually.[304] The ITIF factored potential costs related to hiring data protection officers, conducting privacy audits, and creating data infrastructures into their estimate of adopting a stringent federal data privacy law.[305] In its estimates, the ITIF also attributes 84.8% of the $122 billion worth of economic loss to lowering advertisement effectiveness and lessened access to data for companies.[306]

Another reason for the disapproval of data privacy regulation is that a strict regulation would adversely affect startups, small enterprises, and investment opportunities.[307] While massive companies easily absorb costs related to the GDPR and tighten U.S. data privacy laws, smaller online companies become less competitive within the marketplace because they lack the funding and skill needed to adhere to such laws.[308]

In reality, small businesses are better equipped to comply with data privacy standards and can easily benefit from a transparent legal framework.[309] Because small businesses experience a lesser flow of customers in comparison to multinational companies, there will be less data to collect and transfer.[310] In dealing with less data, small business deal with fewer costs related to maintaining data of customers and clients. Moreover, comprehensive federal data standards would enable small market enterprises to enhance consumer trust between the corporation and client as the client is treated as equals because they have a right to control their personal data and its usage.[311] Furthermore, a GDPR-like framework would allow

302. NEW AMERICA, *supra* note 299.
303. Alan McQuinn & Daniel Castro, *The Cost of an Unnecessarily Stringent Federal Data Privacy Law*, ITIF (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.
304. *Id.*
305. *Id.*
306. *Id.*
307. Jennifer Huddleston, *The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More*, AM. ACTION F. (June 3, 2021), https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more.
308. *Id.*
309. Nigel Jones, *How Small Businesses Can Benefit From the GDPR*, THE PRIV. COMPLIANCE HUB (Apr. 2018), https://www.privacycompliancehub.com/gdpr-resources/how-small-businesses-can-benefit-from-the-gdpr.
310. *Id.*
311. Paula Bruening, *Crafting a Federal Privacy Law to Benefit Small Businesses*, BLOOMBERG L. (Oct. 5, 2020), https://news.bloomberglaw.com/privacy-and-data-security/crafting-a-federal-privacy-law-to-benefit-small-businesses.

small businesses to engage in business in the EU and areas around the globe because it would increase the likelihood of the U.S. obtaining an adequacy decision and favorable treatment from data privacy-focused countries.[312]

Nevertheless, businesses are most concerned with the financial implications of new regulations. Thus, my proposal for establishing a federal framework not only suggests including provisions protecting an individual's data privacy rights through implementing requirements regarding personalized notices, data breach disclosures, and a private right of action but also suggests that the government should offer tax breaks to reduce the financial burden on companies and create a safe and economically beneficial environment for both companies and individuals.

H.R. 1816 partially applies this principle of supporting businesses by offering a small business audit exception.[313] The exception provides that small businesses that deal with the sensitive information of fewer than 250,000 people per year will not be subject to auditing standards.[314] However, this venture would not solve problems related to companies establishing data privacy systems and looking to comply with privacy laws because small enterprises would still incur substantial costs without support. Furthermore, H.R. 1816's business audit exception would fail in protecting the rights of data subjects because it destroys a system of accountability within small businesses as audits are meant to ensure that information is protected and used appropriately.[315]

The best solution is to offer tax credits to companies based on their compliance, yearly audit reports, and overall economic performance. For large corporations that have already set up data privacy systems to comply with the GDPR, there should be a minimal tax credit based solely on audit reports and overall compliance within the company as these companies are able to absorb costs related to audits and data compliance.[316] The minimal tax credit would encourage the data privacy departments of large companies to continue to comply with federal policies and maintain refined standards within their corporations. Meanwhile, a multi-tiered tax credit based on company size, compliance, yearly audit reports, and economic performance related to the circulation of data for small to mid-sized businesses would ease the transition of companies to become data-compliant, while offering incentives that would offset implementation costs.

Data privacy's objective is to ensure that data is handled properly by regulating a data controller's collection, use, and transfer of data, and to assure that an individual's right to privacy is not violated.[317] In a globalizing world that heavily relies on data transfers, the United States has yet to establish a national framework which has caused individuals to distrust businesses and led to companies losing revenue globally. The solution to the United States' data privacy problems is simple: establish a GDPR-like national standard that protects individuals' sensitive information and enables companies to fully enjoy the benefits of unrestricted cross-border transfers of data. If the United States were to do so, the U.S. should reference data

312. *Id.*
313. H.R. 1816, 117th Cong. § 3(a)(6)(C) (2021).
314. *Id.*
315. Kristen Bialik, *Why You Need a Data Audit and How To Conduct It*, CAPTERRA (June 18, 2019), https://www.capterra.com/resources/how-to-conduct-a-data-audit.
316. Mitchell Noordyke, *Big Tech's Shift to Privacy*, IAPP (Oct. 2019), https://iapp.org/resources/article/big-techs-shift-to-privacy-2.
317. *5 Things You Need to Know About Data Privacy*, DATA PRIV, MANAGER (May 16, 2022), https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy.

protection laws in other countries and implement a comprehensive law that adheres to U.S. ideals. Without a national standard, U.S. involvement in global trade and commerce will experience difficulties and American companies will continue to incur unnecessary costs. Therefore, it is time to take a page from the book of global data privacy and implement a national standard.