North Carolina Banking Institute

Volume 24 | Issue 1 Article 21

3-1-2020

United States Data Privacy Law: The Domino Effect After the GDPR

Elizabeth L. Field

United States Data Privacy Law: The Domino Effect After the GDPR

I. INTRODUCTION

Data privacy is a growing and evolving topic.[1] Breaches and significant hardware vulnerabilities leave consumers' personal information susceptible to financial crime and identity theft, moving the issue to the forefront of today's legislation.[2] Recently in the U.S., state data privacy laws have begun to follow the European Union's trend of stricter privacy and cybersecurity regulations and, as a result, are changing the landscape of the banking and financial services industry.[3] The trend began in April 2016 when the European Union ("EU") finalized the General Data Protection Regulation ("GDPR"), which went into effect in May 2018 and focused on the protection of individuals and their personal data.[4]

The GDPR was designed to both prevent data breaches via stricter regulation and tighten the data security protocols used by many companies.[5] The GDPR focused on five main areas: "(1) requiring companies to write clear and straightforward privacy policies; (2) requiring companies to receive affirmative consent from customers before the company can utilize the customer's data; (3) encouraging

---

1. *See* Lisa Hawk, *Data Privacy Day 2018: Data Breaches, Harm, and Culture, Privacy Watch*, BLOOMBERG LAW: LAW REPORTS 1 (Jan. 29, 2018) (describing the growing importance of data privacy).

2. *See id.* (outlining data security and consumer concern).

3. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1; *see also Data Security Law: Private Sector*, (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/86DQ-EJEH] [hereinafter EU General Data Protection Regulation (GDPR)] (describing the U.S. state data privacy policy since 2016 and the increased concern for consumer information).

4. *See* EU General Data Protection Regulation (GDPR), *supra* note 3 (paraphrasing the "protection of natural persons with regard to the processing of personal data and on the free movement of such data"); *see also Data Security Law: Private Sector*, *supra* note 3, at 1 (emphasizing the significant increase in U.S. data privacy security since the passage of the GDPR).

5. *Data Security Law: Private Sector*, *supra* note 3, at 1–2.

companies to increase transparency in how and why user data is transferred, processed, and used in automated decisions; (4) providing data subjects more rights over their data; and (5) granting the European Data Protection Board strong enforcement authority."[6] Because of the GDPR's broad nature, the regulation directly affects U.S. financial institutions, large and small.[7] These financial organizations frantically changed privacy systems and cybersecurity plans to meet GDPR compliance before it took effect in May 2018.[8] As of February 2020, many entities are still struggling to meet all GDPR obligations.[9] Despite the challenges posed by the GDPR,[10] however, U.S. states seem to be quickly following in the EU's path of increased cybersecurity regulation, though not every state includes direct coverage of financial institutions in its legislation.[11]

This Note proceeds in five parts. Part II outlines the GDPR and its impact on U.S. financial institutions.[12] Part III examines U.S. state legislation that mirrors the GDPR's strict data privacy regulation and increased consumer protection and surveys state statutes that have been enacted since GDPR.[13] Part IV discusses the possibility of more state legislation and how such policy could affect the financial world.[14] Furthermore, Part IV will discuss the prospect of a unified federal policy that tightens data privacy security measures taken by corporations.[15]

---

6. *See Data Security Law: Private Sector*, *supra* note 3, at 1 (outlining the GDPR's main goals); Lindsay A. Seventko, Note, *GDPR: Navigating Compliance as a United States Bank*, 23 N.C. BANKING INST. 201, 202 (2019) (describing the main areas of the GDPR).

7. *See* Monica Meinert, *GDPR: These Four Letters Could Spell a Compliance Headache for Smaller Banks*, ABA BANKING J. (Feb. 23, 2018), https://bankingjournal.aba.com/2018/02/gdpr-these-four-letters-could-spell-a-compliance-headache-for-smaller-banks/ [https://perma.cc/9DTJ-CLPU] (outlining the challenges and effects for the GDPR for financial institutions); *see generally* AJ Dellinger, *A Year Later, Many Sites Are Still Failing to Meet Basic GDPR Requirements*, FORBES (May 31, 2019, 10:41 PM), https://www.forbes.com/sites/ajdellinger/2019/05/31/a-year-late [https://perma.cc/6PPH-NQ3U] (outlining effects of the GDPR on covered institutions and the challenges that those businesses are facing).

8. Dellinger, *supra* note 7.

9. *Id.*

10. *Id.*

11. *See Data Security Law: Private Sector*, *supra* note 3 (outlining new data privacy legislation).

12. *See infra* Part II.

13. *See infra* Part III.

14. *See infra* Part IV.

15. *See infra* Part IV; *see also* Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. Part I (2020) (outlining the importance of federal data privacy policy).

II. THE GDPR AND ITS EFFECT ON THE UNITED STATES FINANCIAL SYSTEM

A. The GDPR: A Brief Overview

After taking effect in 2018, the GDPR overhauled the way corporations protect and utilize consumer personal data.[16] The regulation significantly changes the function and reach of data privacy law by broadening its jurisdiction, as well as "what is covered materially" in the law.[17] Furthermore, by allowing EU residents and citizens to sue corporations beyond the EU's borders for violations of the statute, the GDPR's jurisdiction extends far beyond Europe.[18] Unlike the EU's previous leading data privacy policy, the Data Protection Directive, the GDPR applies to corporate entities outside of the European Union.[19] If the company utilizes or retains consumer information in one of its branches located in the EU, it falls under the GDPR regardless of where the data is actually processed.[20] The regulation also extends to any company which monitors the behaviors of or offers goods and services to EU individuals.[21] Because the personal data collected by U.S. financial institutions could belong to European individuals, these organizations fall solidly within the reach of the GDPR.[22]

The EU regulation also redefines "personal data" broadly to cover anything that could identify a "data subject" or individual.[23] This broad definition includes information shared on social media, IP addresses, and

16. *See* Meinert, *supra* note 7 (outlining the effects of the GDPR on small U.S. banks).

17. *Id.*

18. *Id.*

19. *See* EU General Data Protection Regulation (GDPR), *supra* note 3 at 32-33 (outlining which entities the GDPR covers).

20. *Id.* at 33.

21. *Id.* (offering goods/services that are either paid for or for free, or monitoring the behavior of individuals in the EU).

22. *See* Oran Gelb & Joseph Ninan, *GDPR and Financial Institutions: The Top Five Issues*, BRYAN CAVE LEIGHTON PAISNER (May 25, 2018), https://www.bclplaw.com/en-US/thought-leadership/gdpr-and-financial-institutions-the-top-five-issues.html [https://perma.cc/W4ET-SPDR] (describing GDPR provisions and its U.S. consequences); *see also* Pulina Whitaker et al., *GDPR's New Requirements: What Investment Managers, Funds, Banks, and Broker-Dealers Need to Know*, BLOOMBERG LAW (Apr. 17, 2018) (outlining how the U.S. financial sector is impacted by the GDPR).

23. EU General Data Protection Regulation (GDPR), *supra* note 3, at 33 (defining data subjects as identified or identifiable persons to which the personal data relates).

other virtual data.[24] The GDPR's focus on individual rights—another groundbreaking change in EU data privacy policy—provides individuals with greater control over their personal data.[25] In particular, the GDPR includes the right to erasure, otherwise known as the right to be forgotten, as well as the right to data portability.[26]

Overall, the GDPR establishes broad parameters for companies with the personal data of any EU citizen or resident, ultimately creating new regulatory and compliance issues for banks and other corporate entities around the world.[27] In particular, the broad definition of personal data, the new incorporation of personal rights, and the extra-territorial reach of the EU law each pose unchartered challenges for US financial institutions.[28] Major considerations for banks, broker-dealers, investment managers, funds, and other monetary entities include creating processes to categorize information on why it was obtained, determining how to satisfy storage limitations that factor in individual rights, and establishing policies and procedures to follow regulatory requirements or consumer data requests.[29] The GDPR leaves the financial industry grappling with its complicated compliance demands and consumer-focused provisions.[30]

B. The GDPR's Impact on U.S. Banks

The first step in complying with the GDPR is to understand which organizations the law covers.[31] The GDPR applies to organizations that are established in the EU and process EU subjects' personal data, or are established outside of the EU and process personal data in connection with offering goods and services in the EU or that monitor their behavior,

24. *See* Meinert, *supra* note 7 (including information such as IP addresses, social media handles and other pieces of virtual information).

25. *See id.* (outlining the premise that individuals should have control over their personal data).

26. The definition of portability "refers to a data subject's right to request their data from a company and have that data transmitted to another data controller." EU General Data Protection Regulation (GDPR), *supra* note 3, at 42; Meinert, *supra* note 7.

27. *See* Meinert, *supra* note 7 (describing data privacy law compliance issues).

28. *See* Whitaker et al., *supra* note 22 (outlining the GDPR's new provisions).

29. *See id.* (outlining focus areas for financial institutes and GDPR compliance).

30. *See id.* (describing the challenges banks and the financial industry face in regards to the GDPR and data privacy laws).

31. *See* Meinert, *supra* note 7 (describing the importance of understanding which organizations fall under the GDPR).

regardless of where the data processing takes place.[32] When the GDPR took effect, international banks with European offices immediately recognized that the law applied to their businesses because of their geographical presence and obvious collection and use of EU data.[33] Furthermore, financial entities with a large EU consumer base, and thus EU consumer data, presumed that the law included them whether or not they maintained EU-based office locations.[34] Ultimately, while there is no threshold for GDPR application, it is in the best interest for any financial corporation that retains EU data to amend its data processing systems and compliance procedures.[35]

While it is easier for big financial institutions to determine that the GDPR applies to them directly, smaller financial institutions struggle with understanding whether or not the law includes them.[36] For example, a modest community bank in Idaho ordinarily would not be concerned with or learn about European laws because it has little to no interaction or relationship with the EU.[37] The GDPR, however, changed this relationship by opening up potential compliance concerns for small U.S. banks through its broad territorial scope outside of the EU's borders.[38] Fortunately, the EU has directly addressed the question of applicability for small and medium-sized enterprises ("SMEs") by clarifying that businesses which do not process consumer data as a main function of their business and do not pose data privacy risks for individuals, do not need to comply with all GDPR provisions.[39] As a first step, SMEs and other businesses struggling to determine whether they fall under this criteria

32. *See* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKERHOSTETLER LLP, https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [https://perma.cc/V85W-LWTD] (detailing various GDPR provisions while also comparing it to the CCPA); *see also* EU General Data Protection Regulation (GDPR), *supra* note 3, at 2 (paraphrasing the application of the GDPR and its robust coverage).

33. *See* Penny Crosman, *Large U.S. Banks Scramble to Meet EU Data Privacy Rules*, AM. BANKER (Apr. 16, 2018, 1:15 PM), https://www.americanbanker.com/news/large-us-banks-scramble-to-meet-eu-data-privacy-rules [https://perma.cc/3HB3-P4GP] (outlining GDPR coverage); *see also* Whitaker et al., *supra* note 22 (describing the effects of the new GDPR provisions and heightened data privacy security on the U.S. financial sector).

34. Whitaker et al., *supra* note 22.

35. *Id.*

36. *See* Meinert, *supra* note 7 (describing the challenge of understanding the GDPR and what entities are covered by the law).

37. *See id.* (outlining some of the challenges that the GDPR poses to small banking institutions).

38. EU General Data Protection Regulation (GDPR), *supra* note 3 at 31–33.

39. GDPR Key Changes, EUROPEAN UNION, https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/A25U-WR6Q] (last visited Dec. 2019).

should conduct a privacy risk assessment and look at the data regularly collected from their customers in the EU.[40] SMEs in the U.S. should focus on whether they are marketing to, doing regular business with, and collecting the personal data of EU citizens and residents.[41] However, even with additional clarification provided by the EU Commissioner, many small U.S. banks are still unclear as to whether they need to comply with the GDPR and, if so, with which provisions.[42]

Once companies establish that they fall within the GDPR, they often still struggle with compliance issues,[43] including the provision regarding readily accessible privacy policies for consumers.[44] Despite over a year having passed since the GDPR went into effect, more than half of all websites that fall under the GDPR still fail to have a clear and easy-to-find privacy policy for consumers.[45] This failure is surprising because it is one of the easiest compliance pieces of the regulation's requirements.[46]

A second GDPR requirement that remains problematic is complying with rules for tracking cookies.[47] The GDPR requires corporations to reveal if their websites employ cookies to track consumer information and activities online.[48] Organizations are falling short of this requirement in two primary ways: (1) failing to provide a disclaimer that cookies are in use on the site or (2) using insecure cookies to harvest information.[49] Overall, compliance issues are opening websites up to potential data breaches, identify theft, and other harmful events that the GDPR attempts to prevent.[50] Hopefully, as time progresses, all

40. Meinert, *supra* note 7 (recommending a strategy to help SMEs comply with the GDPR).

41. *Id.*

42. *See id.* (describing the uncertainty smaller banks face with the GDPR and providing helpful guidance in hopes of ameliorating confusion).

43. *See* Dellinger, *supra* note 7 (outlining background information of GDPR compliance issues).

44. *See id.* (outlining companies' failure to comply with privacy policies).

45. *Id.*

46. *See id.* (emphasizing the simplicity of providing a clear privacy policy on a business's website).

47. *Id.*

48. *Id.*; *see also* EU General Data Protection Regulation (GDPR), *supra* note 3 at 6 (describing GDPR requirements for consumer data tracking and cookies online).

49. *Id.*

50. Dellinger, *supra* note 7.

organizations and financial institutions will continue to strengthen their data privacy measures and fully adhere to the GDPR requirements.[51]

C. Specific Issues Affecting U.S. Banks

While entities that utilize European resident data struggle to interpret and comply with the GDPR, certain provisions specifically affect U.S. banking institutions.[52] Despite knowing that they fall within the scope of the GDPR, large banks still face challenges imposed by this broad-reaching and complex regulation.[53] First, U.S. banks have invested significantly in updating their systems to be GDPR compliant, with some organizations spending more than $10 million to complete compliance work.[54] One of the largest incentives for these significant investments is the desire to avoid the potential fines imposed for noncompliance, which amount to a maximum of 4% of annual global revenue of the institution.[55] These significant monetary penalties are one of the largest changes to the EU data privacy policy.[56]

Another challenge U.S. banks face is implementing the rules regarding consumer data rights.[57] For example, the right to data portability provides customers with the option to immediately receive a list of all of their personal data that the bank has collected.[58] While this individual right is useful for consumers who wish to know what personal information an organization has on them, it protects more than the traditional data types.[59] Currently, banks can readily access bank account numbers and transaction histories, but this GDPR provision takes data privacy even further by including information about when customers

51. *See id.* (explaining that there is a "long road" before all organizations start valuing data privacy security and the steps taken by the GDPR).

52. *See* Crosman, *supra* note 33 (describing GDPR's effects on financial institutions).

53. *See* EU General Data Protection Regulation (GDPR), *supra* note 3, at 15 (outlining consumer right provisions); *see also* Crosman, *supra* note 33 (describing the right to data portability of data as the ability to "ask for and immediately receive an inventory of all data").

54. *See* Crosman, *supra* note 33 (outlining the significant monetary impacts the GDPR had on financial institutions).

55. *Id.*

56. *Id.*

57. *Id.* at 3.

58. *See* EU General Data Protection Regulation (GDPR), *supra* note 3 at 15 (outlining consumer right provisions); Crosman, *supra* note 33, at 3 (describing the right to data portability of data as the ability to "ask for and immediately receive an inventory of all data").

59. *See* Crosman, *supra* note 33, at 3 (detailing individual rights in the new data privacy laws).

visited the bank's website and what they did on that website.[60] Furthermore, if a bank is capturing cookies and IP addresses of individuals using their sites, it must have the ability to share this information with the customer as well.[61]

The GDPR's right to erasure, also known as the right to be forgotten, presents implementation issues for U.S. banks as well.[62] Consumers are permitted to request that banks remove all information about them, including data that banks typically need to keep for other non-GDPR regulatory purposes, such as other policy requirements that mandate the reporting of consumer information.[63] Additionally, consumer requests must be met within thirty days, which leaves little time for banks to sift through virtual data inventory, backup files, and paper documents.[64] Backup files, which can be extremely difficult to erase, offer another hurdle that prevents complete compliance with the right to erasure.[65] One way banks can offset this challenge and remain compliant with the GDPR, however, is through technological solutions.[66] For example, International Business Machines ("IBM") offers personal data discovery tools that locate and gather consumer data held within a corporation for the costumer or to be erased from the bank's servers.[67]

While on the surface this may seem to solve the problem, these tools do not provide a simple and complete solution.[68] For instance, some technology is designed to sort through unstructured data, while other technology focuses only on structured data.[69] Overall, the rights to a data inventory and data erasure pose significant implementation and compliance issues for U.S. banks, and with the GDPR's broad reach, these new policies also extend to data that banks gather from third parties.[70]

---

60. *Id.*
61. *Id.*
62. *Id.* at 4.
63. *See id.* (describing consumer requests for erasure of personal data).
64. *See id.* (detailing the challenges to consumers' right to erasure).
65. *See id.* (outlining some of the difficulties with advanced technology and erasing consumer data).
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *See id.* (describing the complicated challenges the GDPR poses for financial institutions and consumers' right to erasure).

Finally, the security requirements of the GDPR also pose unprecedented challenges to financial institutions because of their emphasis on data protection.[71] These required security measures include the encryption of personal data, the controlling and monitoring of who can access and use information, and the preparing of a cybersecurity breach readiness plan.[72] Banks must also now notify regulators of breaches within seventy-two hours, which is an incredibly difficult task for most organizations.[73] Furthermore, failure to comply with these costly and burdensome plans means the banks may be stuck paying significant penalty fines.[74]

III. IS U.S. STATE POLICY FOLLOWING IN THE EU'S FOOTSTEPS IN DATA PRIVACY AND CONSUMER PROTECTION?

In enacting the GDPR, the EU took a large and unprecedented leap in data privacy law, especially in regard to territorial scope, broader definitions of personal data, and increased individual consumer rights.[75] The GDPR has triggered a domino effect of U.S. state legislatures enacting consumer protection and data laws.[76] As of May 2019, at least twenty-five states have enacted laws addressing the data security practices of private sector entities, a number which has doubled since 2016 when the EU finalized the GDPR.[77] Most of this state legislation requires businesses that "own, license, or maintain" personal data about a resident of that state to create reasonable security procedures and practices.[78] Through these regulations, states place a heavy emphasis on the protection of personal information in a manner similar to the GDPR.[79] Further paralleling the GDPR, more than half of these states focusing on

71. *Id.* at 5.

72. *See id.* (outlining GDPR breach notification provisions).

73. *See id.* (explaining that the average time for most organizations to realize there is a data privacy breach is 100 days).

74. *Id.*

75. EU General Data Protection Regulation (GDPR), *supra* note 3, at 32–33; *see generally* Whitaker et al., *supra* note 22 (outlining how the new, expansive GDPR provisions will affect the financial sector).

76. *See Data Security Law: Private Sector*, *supra* note 3, at 1 (outlining the new U.S. legislation focused on increasing data privacy security for consumers).

77. *See id.* (describing the growing concern for data privacy and the consequential increase in data privacy policy in the U.S.); *see generally* EU General Data Protection Regulation (GDPR), *supra* note 3 (heightening data privacy security for European Union consumers).

78. *Data Security Law: Private Sector*, *supra* note 3.

79. Meinert, *supra* note 7.

privacy laws also enacted data disposal laws, which require financial entities to dispose of certain personal information at the request of the consumer.[80] The trend of increased data privacy regulation continues, with several states closely mirroring the GDPR's philosophy of enhanced consumer protection through increased individual rights and stricter regulation, consequently further complicating banks' compliance and data procedures.[81]

A. The California Consumer Privacy Act of 2018

On June 28, 2018, California Governor Jerry Brown signed Assembly Bill 375, enacting what is now known as the California Consumer Privacy Act of 2018 ("CCPA").[82] The new policy, which went into effect in 2020,[83] strikingly mirrors the GDPR in several ways, making it the most notable state data privacy legislation.[84] The GDPR protects data subjects,[85] or individuals who are in the Union, regardless of nationality or residence.[86] The CCPA, on the other hand, applies to the personal information of a California "consumer" and "resident," [87] defined more narrowly as "(1) every individual who is in California for other than a temporary or transitory purpose, and (2) every individual domiciled in California who is outside the State for a temporary or transitory purpose."[88] Both laws focus on information regarding an

80. *See Data Security Law: Private Sector*, *supra* note 3, at 1 (outlining states' data privacy laws).

81. Jehl & Friel, *supra* note 32.

82. California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100 (West 2018); *see also* Lauren Davis, Note, *A Quick Alteration from Past Privacy Acts or a Major Change? How the California Consumer Privacy Act Effects Financial Institutions Across the Nation*, 24 N.C. BANKING INST. Part I (2020) (describing the CCPA and how it affects the financial industry).

83. CAL. CIV. CODE § 1798.100 (West 2018).

84. EU General Data Protection Regulation (GDPR), *supra* note 3; *see also* Lauren Davis, Note, *A Quick Alteration from Past Privacy Acts or a Major Change? How the California Consumer Privacy Act Effects Financial Institutions Across the Nation*, 24 N.C. BANKING INST. Part I (2020) (outlining the CCPA and its effects on United States financial institutions).

85. EU General Data Protection Regulation (GDPR), *supra* note 3, at 5.

86. *Id.* at 2.

87. CAL. CIV. CODE § 1798.100 (West 2018).

88. *See* Jehl & Friel, *supra* note 32, at 1 (comparing the CCPA and the GDPR); *see generally* CAL. CIV. CODE § 1798.100 (paraphrasing "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

identifiable natural person but differ on how they define such a person.[89] Despite these variations, however, each regulation provides broad coverage and has potential extraterritorial effects on financial institutions outside of their jurisdiction.[90]

Additionally, the GDPR and the CCPA cover similar types of information.[91] The GDPR protects "personal data," or "any information relating to an identified or identifiable" data subject,[92] while the CCPA includes "personal information" that identifies, relates to, or is or can be linked to a specific individual or family.[93] These provisions are substantially similar, with the CCPA also including information linked at the household or device level.[94] Another similarity between these two laws is the emphasis on individual consumer rights.[95] Both regulations include the right of disclosure or access, the right of data portability, and the right to deletion/erasure.[96] Through the protection of these consumer rights, the GDPR and the CCPA are focusing on the consumer's ability to access, transfer, and erase his or her personal information, ultimately decreasing financial institutions' control over data.[97]

Since the passage of the Gramm-Leach-Bliley Act ("GLBA") in 1999, the banking and finance world relied on its exclusive application to financial institutions and other sector-specific legislation, such as the Fair Credit Reporting Act.[98] The CCPA, however, does not include a blanket exemption for financial institutions, but rather exempts only certain individual data that is gathered, processed, sold, or released pursuant to

89. *See* Jehl and Friel, *supra* note 32, at 2 (outlining the meaning of "persons" in data privacy law).

90. *Id.*

91. *Id.*

92. EU General Data Protection Regulation (GDPR), *supra* note 3, at 33.

93. CAL. CIV. CODE § 1798.140(o).

94. Jehl & Friel, *supra* note 32.

95. EU General Data Protection Regulation (GDPR), *supra* note 3; CAL. CIV. CODE § 1798.100.

96. EU General Data Protection Regulation (GDPR), *supra* note 3; CAL. CIV. CODE § 1798.100; *see also* Victoria Finkle, *The States at the Forefront of Consumer Privacy Legislation*, AM. BANKER, 2019, https://www.americanbanker.com/list/the-states-at-the-forefront-of-consumer-privacy-legislation [https://perma.cc/MW3T-SMU4] (describing several state policies that increase data privacy regulation in the U.S.).

97. *See* Jehl & Friel, *supra* note 32 (discussing the similarities between the CCPA and GDPR, both of which are increasing consumer data protection through increased regulation).

98. *See generally* Jehl & Friel, *supra* note 32 (discussing the GLBA and foundation of US finance law).

the federal GLBA.[99] This means that the CCPA could force financial institutions to amend how they collect and utilize consumer data, consequently affecting various forms of consumer lending and credit underwriting.[100] Just as the GDPR left the financial sector scrambling to meet stringent data regulations, the CCPA will similarly affect U.S. banks.[101]

B. The New York "Stop Hacks and Improve Electronic Data Security Act"

Shortly after California passed the CCPA, New York also enacted a comprehensive data privacy protection law, the Stop Hacks and Electronic Data Security Act ("SHIELD Act"), continuing the GDPR domino effect.[102] The SHIELD Act addresses data privacy matters emphasized in the GDPR but differs in its approach to financial institutions.[103]

First, the SHIELD Act amends New York's data breach notification statute by updating its definitions.[104] The amendment expands the definition of "private information" to include personal information such as social security numbers, driver's license numbers, account numbers, biometric information, and user names or email addresses.[105] While not as comprehensive as the GDPR's overarching definition of private data, the SHIELD Act still follows the EU's footsteps by broadening the meaning of personal information.[106] Furthermore, the Act parallels the GDPR in its extra-territorial

99. *See* CAL. CIV. CODE § 1798.145 (describing "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act").

100. Joe Rubin, *Banks Must Brace for Renewed Privacy Fight*, AM. BANKER 53 (Dec. 20, 2018 10:01 AM), https://www.americanbanker.com/opinion/banks-must-brace-for-renewed-privacy-fight [https://perma.cc/AZ42-HYMW].

101. *See* Jehl & Friel, *supra* note 32 (describing the effects and provisions of the GDPR and CCPA and which organizations fall under the two policies).

102. Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), N.Y. GEN. BUS. § 899-aa (2019).

103. *Id*.

104. *Id.*; *see also* F. Paul Greene, *New York SHIELD Act Promises More Data Breach Enforcement, and International Reach*, N.Y. L. J. (July 26, 2019, 12:10 PM), https://www.law.com/newyorklawjournal/2019/07/26/new-york-shield-act-promises-more-data-breach-enforcement-and-international-reach/?slreturn=20190723114318 [https://perma.cc/U8QF-DV87] (describing the New York SHIELD Act and its provisions).

105. SHIELD Act, N.Y. GEN. BUS. § 899-aa(1)(b).

106. *Id.*

application.[107] The SHIELD Act requires any person or business that licenses or owns computerized data of a New York resident to comply with the law's breach notification requirements, regardless of whether the person or organization conducts business within New York itself.[108]

Much like the GDPR, the New York law extends its reach—and therefore its impact—far beyond its geographic borders, creating compliance issues for financial institutions around the country.[109] While the CCPA further mirrored the GDPR through its implementation of individual data rights, the SHIELD Act primarily focuses on its broad jurisdictional reach and stringent data protection requirements based on its new definition of private information.[110] The SHIELD Act also implements penalties for non-compliance, including $20 per failed breach notification with a maximum of $250,000.[111] While the punishments are not as significant as the GDPR, the New York law still follows the trend of enforcing financial institution compliance through strict monetary penalties.[112]

The impact of this increased data regulation on the financial world is still uncertain and evolving.[113] As of now, New York seems to be intentionally leaving the majority of financial data regulation in the hands of the long-established federal GLBA, though banks should still pay attention to the SHIELD Act.[114] The SHIELD Act explicitly exempts organizations that are covered by and in compliance with the GLBA or New York's other leading cybersecurity legislation, but financial institutions will still have to amend information systems holding private information that are not already subject to federal or state law.[115] For example, a bank personnel system which holds private information about its employees will need to independently meet the SHIELD Act's

107. *See id.* (discussing the New York data privacy policies).

108. *Id.*

109. *Id.*; Greene, *supra* note 104 (outlining the effects of the New York SHIELD Act).

110. SHIELD Act, N.Y. GEN. BUS. § 899-aa; Greene, *supra* note 104 (outlining the effects of the New York SHIELD Act).

111. SHIELD Act, N.Y. GEN. BUS. § 899-aa(6)(a).

112. *Id.*; Greene, *supra* note 104 (outlining the effects of the New York SHIELD Act).

113. SHIELD Act, N.Y. GEN. BUS. § 899-aa.

114. *See generally* Greene, *supra* note 104 (outlining the challenges created by the SHIELD Act for financial institutions).

115. *See generally* Rubin, *supra* note 100 (paraphrasing "will need to implement the SHEILD Act requirements as to information systems holding private information"); 23 NYCRR § 500 (2017).

provisions since employees are not included under mandated protections for systems retaining consumer data.[116]

Furthermore, the SHIELD Act's far-reaching effects mean that businesses with any New York resident data should take recommended reasonable safeguards, including implementing administrative, technical, and physical safeguards on covered data.[117] Even though financial institutions are not mandated to notify affected New York residents beyond the requirements of the GLBA or New York cybersecurity regulations, they are still "required to notify the New York attorney general, the New York State Department of State Division of Consumer Protection, and the New York State Division of the State police."[118] Overall, New York financial organizations should consider their existing data privacy and cybersecurity safeguards in light of the risk of breach or non-compliance.[119]

Although New York is already considered to be at the forefront of consumer data protection, the state could potentially further cement this position by passing another data privacy policy, the New York Privacy Act.[120] The current bill is similar to and influenced by the GDPR .[121] New York Senator Kevin Thomas, who sponsored the SHIELD Act, introduced the New York Privacy Act in May of 2019.[122] This new bill resembles the GDPR in its proposed jurisdictional scope, broad definition of personal information, and focus on consumer rights; however, it still excludes personal consumer information that is regulated by the GLBA.[123]

116. *See generally* W. Scott Kim & Alejandro Cruz, *New York's SHIELD Act Heads to the Governor's Desk*, PATTERSON BELKNAP: DATA SECURITY LAW (July 9, 2019), https://www.pbwt.com/data-security-law-blog/new-yorks-shield-act-heads-to-the-governors-desk/ [https://perma.cc/KU97-JD56] (describing the consumer privacy provisions in New York data privacy law).

117. *Id.*

118. *Id.*

119. *Id.*

120. *See id*. (describing the potential New York data privacy law and its effects on consumers).

121. *Id.*

122. S.B. S5642, 2019-2020 Leg. Sess. (N.Y. 2019).

123. *See id.* (paraphrasing "personal data sets to the extent that they are regulated by . . . the Gramm-Leach-Bliley Act of 1999").

C. Other States that Followed GDPR Data Privacy Trends

While California and New York enacted two of the most GDPR-like data privacy laws, several other states have introduced or enacted legislation that incorporates certain aspects of the EU policy as well.[124] One of the most notable pieces of data privacy legislation is Hawaii's Senate Bill 416.[125] Similar to the GDPR, this bill requires financial institutions to disclose certain consumer data sets that are collected, used, sold, or transferred.[126] Furthermore, the bill increases data privacy legislation by providing consumers with the right to request disclosures or deletions of personal information.[127] The Hawaiian law also makes no mention of a GLBA exception.[128]

The Maryland legislature also proposed Senate Bill 418 in February 2019, incorporating similar rights for Maryland residents as those created for California residents in the CCPA and EU residents in the GPDR.[129] This proposed bill requires businesses, including financial institutions and banks, to provide data collection notice to consumers.[130] Furthermore, it allows consumers to submit requests to financial institutions to receive the data collected about them.[131] The Maryland bill also tightens compliance requirements, such as laying out specific procedures for how a financial institution must comply with a consumer's request for the deletion of personal information.[132] The proposal does not fully carve out financial institutions regulated by the GLBA but instead provides a carve-out for those specific data sets that are covered by GLBA provisions.[133]

---

124. *See* Paul Breitbarth, *Keeping on Top of Changes in U.S. Privacy Laws*, ABA BANKING J. (Oct. 31, 2019), https://bankingjournal.aba.com/2019/10/keeping-on-top-of-changes-in-u-s-privacy-laws/ [https://perma.cc/KYT8-NAEK] (describing recent state privacy legislation).

125. S.B. S418, 2019-2020 Leg. Sess. (H.I. 2019).

126. *Id.* at 2.

127. *Id.* at 3.

128. *See id* (outlining state data privacy law).*; see also* Annie Allison and Philip J. Bezanson, *Somebody's Watching EU: Washington State Senate Passes Privacy Legislation Similar to European Union's Data Privacy Regulations*, BRACEWELL LLP (Mar. 12, 2019), https://www.natlawreview.com/article/somebody-s-watching-eu-washington-state-senate-passes-privacy-legislation-similar-to [https://perma.cc/9SQ9-A2UG] (outlining several states with increased data privacy legislation).

129. S.B. S613, 2019 Leg., Reg. Sess. (M.D. 2019).

130. *Id.* at 1.

131. *Id.*

132. *Id.* at 8.

133. *Id.*

Finally, Washington is another state that has pivoted toward GDPR-like legislation.[134] In March 2019, the Washington Senate approved the Washington Privacy Act,[135] addressing the same data privacy concerns outlined in the GDPR.[136] The Washington Privacy Act increases resident consumer rights, including the right to erasure, as well as the jurisdictional scope of its state data privacy legislation.[137] While this bill does not cover all personal information collected from a Washington citizen, it does include the personal information collected by financial institutions that conduct business in Washington or intentionally target Washington residents.[138] Though the Washington bill did not pass the House of Representatives, its prevailing sentiment of GDPR-like legislation is expected to be reintroduced in future sessions.[139]

Other states continue to enact data privacy laws influenced by various parts of the GDPR.[140] While California passed the most cumbersome policy thus far, it will be important for financial institutions to stay on top of ongoing legislation updates and compliance requirements.[141]

IV. UNITED STATES DATA PRIVACY LAW: CONCLUSIONS AND PREDICTIONS

With more states enacting consumer protection rights and strict data privacy policies in recent years, the financial industry will either need to accept these new compliance challenges and stricter regulations or begin to play an active role in the data privacy debates.[142] The GDPR was the first such law to have far-reaching and extensive consequences for U.S. financial services companies, and California led the way stateside.[143] Other states, including New York and Hawaii, also enacted

134. *See* Allison & Bezanson, *supra* note 128 (comparing the Washington Privacy Act to the GDPR).

135. S.B. 5376, 2019 Reg. Sess. (Wash. 2019).

136. *See id.* (outlining the Washington data privacy bill); *see also* Breitbarth, *supra* note 124 (describing the premise behind the Washington data privacy bill).

137. S.B. 5376, 2019 Reg. Sess. (Wash. 2019).

138. *Id.*

139. *See* Breitbarth, *supra* note 124 (describing possible data privacy laws).

140. *See* Finkle, *supra* note 96 (outlining states that enacted laws similar to the GDPR).

141. *See* Breitbarth, *supra* note 124 (explaining the importance of data privacy laws and financial institutions).

142. *See* Finkle, *supra* note 96 (emphasizing the importance of data privacy security and the possibility of new policies).

143. *Id.*

GDPR-like legislation, further continuing the trend.[144] Future consumer protection legislation could continue to extend its regulations to financial entities, thus mirroring the EU law.[145] As new state data privacy laws begin to take effect, unexpected costs, regulatory issues, and enforcement impossibilities may continue posing compliance challenges for financial organizations, large and small.[146]

While state legislatures continue to introduce new data privacy laws, Congress has been considering its own federal reform.[147] The Obama administration laid out a blueprint for its Consumer Privacy Bill of Rights, which included what were termed the "Fair Information Practice Principles."[148] This initiative recognized the importance of individual consumer protection rights, including knowing how one's data is "collected, used, and shared by companies and government entities alike."[149] Obama's proposal lost momentum over time, however, and the Trump administration has focused very little on technology policy.[150]

In 2019, some members of Congress discussed the need to create a unified, federal data privacy law.[151] Further, with the CCPA taking effect in the near future, both Republicans and Democrats recognize the need for a comprehensive federal law to protect consumer privacy.[152] This idea stems from the inconsistent patchwork approach taken by the US, compared to other similarly developed countries which implemented overarching privacy regimes incorporating the EU's GDPR.[153] As more state legislatures pass data privacy laws, the need for federal regulation

144. *Id.*

145. *See id.*

146. *See id.* (outlining possible future compliance challenges for U.S. financial institutions).

147. *Id; see also* Soubouti, *supra* note 15 (discussing federal data privacy laws and possible ramifications for the financial industry).

148. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL.: DIGITAL AND CYBERSPACE POL'Y PROGRAM (Jan. 20, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/U5ZV-B2U3].

149. *Id.*

150. *Id.*

151. *See* David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It is Nowhere in Sight*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html [https://perma.cc/5SJ9-DNF5] (describing talks of a federal data privacy law).

152. *See id.* (outlining U.S. politician positions on a federal data privacy regulation).

153. *See id.* ("Privacy regimes that are compatible with the EU's GDPR rather than with the patchwork approach.").

only increases.[154] Nonetheless, a unified and comprehensive federal data protection policy could wreak havoc on financial institutions that utilize complicated systems for processing customer information.[155]

ELIZABETH L. FELD*

154. *See id.* (describing the concerns with enacting various state policies).

155. *See* O'Connor, *supra* note 148 (outlining possible consequences of a federal data policy in the United States).

* I would like to thank my family for their unwavering support and understanding throughout the development of this Note. I am also incredibly grateful to Professor Lissa L. Broome, Brianne Marino Glass, Brad Cheek, and the staff members of the North Carolina Banking Institute Journal for their thoughtful guidance and edits during the publication process.