NEW YORK'S PUSH TO CONSUMER DATA PRIVACY: STATE LEGISLATION MAY BE HERE TO STAY

Patrick Mullery[†]

ABSTRACT

The digital age has given rise to global technology usage with millions of daily users. Big technology companies can monetize user

[†] J.D. Candidate, Syracuse University College of Law, Class of 2024. Special thanks to the community of Syracuse University and the members of Syracuse Law Review for their insight, dedication, and encouragement.

data by storing, analyzing, and interpreting data to build specific data profiles on a user-by-user basis. There are constantly new and inventive ways companies collect data, making it difficult for lawmakers to keep up with the highly innovative market space. Legislators around the globe have been trying to protect personal data by enacting, or attempting to enact, laws to provide people with the fundamental right of personal data privacy protection.

The European Union took a monumental step forward in data regulation by enacting the General Data Protection Regulation in 2018. The General Data Protection Regulation's fundamental goal is to protect personal data and provide rules, restrictions, and guidelines for how technology companies may use this data. Nearly four years later, the United States attempted to follow suit on a federal level with the American Data Privacy and Protection Act.. This bill would have given American citizens the right to personal data privacy and provide guidelines, restrictions, and regulations to companies on how they may use the personal data of their consumers. This bill would have created a uniform law throughout the United States by preempting state-enacted data privacy legislation with an included carve-out for state laws that offer a higher degree of protection, such as the California Privacy Rights Act and Illinois' Biometric Information Privacy Act. However, due to Congress' standstill and failure to pass a sweeping bill, data privacy protection in the United States varies on a state-by-state basis with some federal intervention in specific fields. California is at the forefront of state consumer data privacy laws and has enacted the California Consumer Privacy Act, later amended by the California Privacy Rights Act, offering enhanced personal data protection for consumers in the state of California.

As part of the developing legislation throughout the United States, New York is conceivably in the process of enacting the New York Privacy Act offering enhanced personal data privacy protection to consumers in the state of New York. The political landscape has been slow to move, but there has been public pressure and a pressing need to give consumers the protection they deserve. New York should seek to enact the New York Privacy Act S365, with some revisions, regardless of potential federal legislation on the horizon because New Yorkers should be afforded proper personal data privacy protection while giving companies clear and comprehensive guidelines.

INTRODUCTION

The internet and smart phones have revolutionized the world. People utilize powerful technology every single day with access at

their fingertips. The growth of technology has improved many aspects of people's lives, including how people socialize, do business, and communicate with one another.[1] However, these great technological advancements are not all sunshine and rainbows. There are many negative externalities associated with such a reliance on the internet. Powerful companies who helped establish what the internet is today, including Google and Facebook, track data on their users.[2] This data includes what people search for, where people go, and who people talk to—generating massive data compositions of each individual user.[3] This data can then be used for targeted ads and sold to third parties to be used in a variety of manners.[4] There is no shortage for a market of this data either. The worldwide revenue for digital advertising was $465.5 billion in 2021 and is expected to grow to $683.1 billion through 2026.[5]

Companies collecting user data to turn a profit can raise many concerns for consumers—it can be considered an invasion of a user's right to privacy. Many users may feel data privacy has a direct correlation with freedom of association, freedom of speech, and even human dignity.[6] Legislators have been listening to these concerns and have been enacting laws to protect consumer data privacy.[7] The European Union (EU) led the charge by enacting the General Data Protection Regulation (GDPR) in 2018.[8] The United States attempted to slowly follow suit with the American Data Privacy and Protection Act (ADPPA).[9] However, due to Congress' standstill and failure to pass a sweeping bill, data privacy protection in the United States is currently

1. AMNESTY INT'L, SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS 5 (2019), https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

2. *Id.* at 6.

3. *Id.*

4. *Id.*

5. *Digital Advertising: Market Data & Analysis*, STATISTA (Dec. 2021), https://www.statista.com/study/42540/digital-advertising-report/.

6. *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, GLOB. INTERNET LIBERTY CAMPAIGN, https://gilc.org/privacy/survey/intro.html (last visited Oct. 7, 2023).

7. *Id*.

8. *See* 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), 2 [hereinafter GDPR].

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

controlled on a state-by-state basis with some federal intervention in specific fields.[10] Certain states have robust consumer data privacy laws offered to their residents, with other states falling far behind.[11] New York should seek to enact the New York Privacy Act S365 (NYPA), with some revisions, regardless of potential federal legislation on the horizon because New Yorkers should be afforded proper personal data privacy protection while giving companies clear and comprehensive guidelines.

Part I will briefly discuss what the GDPR is, who the GDPR protects, and how the GDPR offers data privacy protection to consumers. Though enacted in the EU, the GDPR has a cascading effect on American companies, users, and politicians. It is important to understand how the GDPR has affected companies' operations and how it has made an impact on legislatures in the United States.

Part II will discuss the previously proposed ADPPA and the current federal laws in the United States focused on consumer data privacy. This Note will detail how the ADPPA would have impacted companies, how it would have been enforced, preemption of state laws, private right of action, and potential advantages and drawbacks associated with the previously proposed legislation.

Part III will discuss the current landscape of state-enacted data privacy laws. This Note will highlight the most impactful state laws that affect companies' operations, most notably California and Illinois.

Part IV will discuss the proposed NYPA. This Note will detail the scope of the legislation, who it seeks to protect, who must abide by it, enforcement, and potential remedies. Finally, this Note will critique the NYPA suggesting a modified version and recommend the bill should be passed regardless of potential federal preemption on the horizon.

I. GENERAL DATA PROTECTION REGULATION

On May 25, 2018, the GDPR officially went into effect in the EU.[12] The GDPR's main objective is to set guidelines and regulations

10. 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/.

11. *47 States Have Weak or Nonexistent Consumer Data Privacy Laws*, SECURITY.ORG (Aug. 31, 2023), https://www.security.org/resources/digital-privacy-legislation-by-state.

12. *The History of General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Sept. 20, 2023).

relating to the "processing of personal data and rules relating to the free movement of personal data."[13] The GDPR seeks to protect the fundamental rights and freedoms of people in the EU, and in particular, their right to the protection of their personal data.[14]

A. GDPR's Implication on Consumer Data

The GDPR protects individuals located in the EU, regardless of citizenship or length of stay.[15] With a broad range of protection, the GDPR has a major impact on companies either established in the EU or conducting business within the EU. There are two major principles companies must abide by as to whether the GDPR applies to them.[16] First, "if the processing of personal data takes place in the context of the activities of an establishment or organization in the EU, regardless of whether the processing itself takes place in the EU," then the regulation applies.[17] Second, "if the personal data of individuals who are in the EU is processed by an organization not established in the EU and the processing concerns the offering of goods or services to individuals in the EU, or monitoring the behavior of individuals that takes place in the EU," then the regulation also applies.[18] If a company meets one of those criteria, irrespective of the size and whether its activity is for profit or not, it must conform to the GDPR's regulations.[19] The latter of the two major principles encompasses many U.S. companies conducting business in the EU, and these companies must be aware of the GDPR's application to their operations.

B. Obligations of Companies Under the GPDR

The GDPR lays out many regulations for data controllers, a category many U.S. companies may fall under. The GDPR defines a data controller as "a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines

13. GDPR*, supra* note 8.

14. *Id*.

15. Madeline M. Cook, *Bringing Down Big Data: A Call for Federal Data Privacy Legislation*, 74 OKLA. L. REV. 733, 764 (2022); *see also* Matthias Artzt, *Territorial Scope of the GDPR From a US Perspective,* INT'L ASS'N OF PRIV. PROS. (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/.

16. Artzt, *supra* note 15.

17. *Id.*; *see also* GDPR*, supra* note 8.

18. Artzt, *supra* note 15.

19. Cook, *supra* note 15, at 764; *see also GDPR vs. CCPA: Crucial Differences You Need To Know*, WIREWHEEL (Dec. 9, 2019), https://wirewheel.io/blog/differences-between-ccpa-gdpr-dsar/.

the purposes of any personal data and the means of processing it."[20] Data controllers decide how personal data is used and processed, so controllers must abide by most of the GDPR's regulations.[21]

The GDPR contains forty-five regulations directly related to data collection and processing practices.[22] While this list may seem exhaustive, there are a few important practices companies must abide by. "First, [data] controllers must obtain consent from data subjects to process their data."[23] Data subjects are defined as an identified or identifiable natural persons in the EU, and this "consent must be communicated through clear terms, freely given by the user, and revocable at any time."[24] Second, "if data subjects request their data profile . . . the controller must provide them with a free copy of all of the data . . . and explain how that data is being used."[25] Third, "because the GDPR gives data subjects the 'right to be forgotten,' controllers must be prepared to remove data in response to valid requests."[26] Finally, "data controllers should build their systems to [incorporate] 'privacy by design'—[privacy by design] . . . include[s] measures to minimize the amount of personal data being processed, process[ing] [of] personal data in a way that prevents it from being attributed to a particular individual, or allow[ing] data subjects to monitor the processing of their data."[27]

C. Enforcement & Remedies

Each Member State must appoint a Data Protection Authority (DPA) responsible for monitoring and enforcing the GDPR.[28] The DPA has several powers, including an order to end a violation, an

20. *GDPR Data Controllers and Data Processors*, GDPR EU, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ (last visited Sept. 20, 2023).

21. *GDPR vs. CCPA: Crucial Differences You Need To Know*, *supra* note 19; *see also* Cook, *supra* note 15, at 765.

22. Cook, *supra* note 15, at 765; *see also* Roslyn Layton & Julian McLendon, *The GDPR: What It Really Does and How the U.S. Can Charter a Better Course*, THE FEDERALIST SOC'Y (Oct. 29, 2018), https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.

23. Cook, *supra* note 15, at 765.

24. *Id.*; *see also* GDPR, *supra* note 8, at 4.

25. Cook, *supra* note 15, at 765–66.

26. *Id.* at 766.

27. *Id.*

28. *See* Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement,* CTR. FOR STRATEGIC AND INT'L STUD. (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement.

instruction to adjust the data processing to comply with the GDPR, as well as the power "to impose a temporary or definitive limitation including a ban on data processing."[29] DPAs may assess fines for specific data protection violations in accordance with the GDPR.[30] The fines are applied in addition to, or instead of, further remedies or corrective powers.[31]

One of the largest fines to date under the GDPR is against Amazon.com, Inc. (Amazon).[32] On July 16, 2021, the Luxembourg National Commission for Data Protection (CNDP) issued a fine against Amazon for a violation of the GDPR in the amount of €746 million ($888 million).[33] By May 2018, over 10,000 people filed a complaint against Amazon "through a French privacy rights group that promotes and defends fundamental freedoms in the digital world."[34] "The CNPD opened an investigation into how Amazon processes personal data of its customers and found infringements regarding Amazon's . . . [targeted advertising] system that was carried out without proper [user] consent."[35]

Enforcement remedies may deter companies from violations, but some people critique the GDPR and its potential fines. Established technology companies, like Amazon, can withstand significant fines, including the $888 million fine issued against them.[36] However, smaller technology companies may not be able to afford such a costly fine.[37] Critics claim that "instead of using fines to deter the companies . . . doing the most damage in terms of online data privacy, the GDPR has the potential to further strengthen the largest technology companies' existing monopolies by wiping out their competition" who cannot afford such large fines.[38]

The EU has established comprehensive legislation coupled with large fines for its citizens, but data compilation of users can occur anywhere in the world.[39] The GDPR has inspired lawmakers around the

29. GDPR, *supra* note 8, at Art. 58.
30. *Id.*
31. *Id*.
32. *20 Biggest GDPR Fines So Far [2023],* DATA PRIVACY MANAGER (Sept. 19, 2023), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020.
33. *Id.*
34. *Id.*
35. *Id.*
36. Cook, *supra* note 15, at 767.
37. *Id.*
38. *Id.*
39. *Id.*

world to enact data privacy regulations, including the United States.[40] While the United States has impactful state laws protecting consumer data privacy accompanied by several industry specific federal laws,[41] the United States seeks to potentially enact federal legislation giving overarching and uniform guidelines to companies with the goal to offer national consumer data privacy protection.[42]

II. AMERICAN DATA PRIVACY & PROTECTION ACT

Following the GDPR, the world is making a push for enhanced personal data privacy protection, including the United States.[43] The ADPPA was introduced on June 21, 2022, by Representative Frank Pallone which was referred to the Committee on Energy and Commerce.[44] The ADPPA was an overarching act that would have created many new regulations for companies operating in the U.S. If successful, the act would have:

> [I]mpose[d] broad data collection and data processing requirements on a . . . [variety] of covered entities;[45] give[n] individual consumers [the right] to access, correct, and delete . . . personal data; prohibit[ed] companies from using data . . . that discriminates against protected classes;[46] and require[ed] companies to submit annual impact assessments regarding how their algorithms work.[47]

A. Current Federal Laws on Data Privacy

With the previously proposed ADPPA in mind, it is important to consider the current federal laws already established offering consumer data privacy. These federal laws only protect specific types of data in specific circumstances.[48] For example, the Health Insurance Portability and Accountability Act (HIPAA) covers communication between a person and that person's "covered entities, which

40. *Id.* at 769.

41. Klosowski, *supra* note 10.

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

43. *See generally id.* (explaining the details of the H.R. 8152); *see Shaping a Safer Digital Future: A New Strategy for a New Decade*, EUROPEAN DATA COLLECTION SUPERVISOR, https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en (last visited Jan 11, 2024).

44. *Id*.

45. Cook, *supra* note 15, at 775.

46. *Id*.

47. *Id*.

48. Klosowski, *supra* note 10.

includes doctors, hospitals, pharmacies, insurers, and other similar businesses."[49] The Gramm-Leach-Bliley Act (GLBA) "requires consumer financial products, such as loan services or investment-advice services, to explain how they share data, as well as the consumer's right to opt out."[50] The law does not restrict how companies use the data they collect, as long as they disclose such usage prior.[51] The Federal Trade Commission Act (FTC Act) empowers the FTC to pursue an application or website that violates its own privacy policy.[52] Though these laws are important, they are not as encompassing as the ADPPA and provide minimal protection in only specific circumstances. The United States sought to fill the gaps of current federal data privacy laws through the previously proposed ADPPA.[53]

B. American Data Privacy & Protection Act – Goals & Enforcement

The ADPPA had several objectives, including establishing requirements for how companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual.[54] The ADPPA aimed to prohibit companies from transferring individuals' personal data without their affirmative express consent; establish consumer data protections, including the right to access, correct, and delete personal data;[55] provide additional protections with respect to personal data of individuals under the age of seventeen and further prohibit companies from using personal data to discriminate based on specified protected characteristics;[56] and to preempt state laws that are covered by the provisions of the bill except for certain categories of state laws and specified laws in California and Illinois.[57]

The ADPPA would have primarily been enforced by the Federal Trade Commission (FTC), allowing the FTC to institute a civil action for any violation of the ADPPA.[58] Additionally, a state Attorney

49. *Id*.
50. *Id*.
51. *Id*.
52. *Id.*
53. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).
54. *Id*.
55. *Id*.
56. *Id*.
57. *Id*.
58. *American Data Privacy Protection Act ("ADPPA"): Is the U.S. Finally Getting Federal Data Privacy Protection?,* DAC BEACHCROFT (Sept. 30, 2022), https://www.dacbeachcroft.com/es/gb/articles/2022/september/american-data-

General may not file its own suit on behalf of a nationwide class of consumers, but rather, an Attorney General of any implicated state may choose to interview in the FTC action.[59] The ADPPA "would [have] also require[d] the FTC to create a new Bureau of Privacy and a separate fund in the United States Treasury called the Privacy and Security Victims' Relief Fund."[60] Moreover, violations of the ADPPA would have constituted as "deceptive practices" under the FTC Act and may have enabled recovery of damages, civil penalties, restitution, and attorneys' fees and costs.[61]

C. Preemption, Carve Out, & Private Right of Action

The current landscape of data privacy laws in the United States are mainly dictated by state regulations.[62] The ADPPA aimed to set a national standard for privacy by superseding the existing patchwork of state laws through preemption.[63] However, there were explicit carve-outs for existing state legislation, including state legislation in California and Illinois.[64] The ADPPA stated:

> No State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.[65]

The language used in the ADPPA indicates that the drafters of the bill intended express preemption of the current state laws.[66] The bill went on to say:

> Paragraph (1) may not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements: . . .

---

privacy-protection-act-adppa-is-the-us-finally-getting-federal-data-privacy-protection/.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. Hirsh Chitkara, *The Federal Privacy Bill Might Be a Sheep in Wolf's Clothing,* PROTOCOL (Aug. 31, 2022), https://www.protocol.com/newsletters/policy/privacy-preemption-adppa?rebelltitem=10#toggle-gdpr.

64. *Id.*; *See also* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

65. H.R. 8152 § 404.

66. *Id.*

> (M) The Biometric Information Privacy Act (740 ICLS 14 et seq.) and the Genetic Information Privacy Act (410 ILCS 513 et seq.) . . .
>
> (R) Section 1798.150 of the California Civil Code (as amended on November 3, 2020, by initiative Proposition 24, Section 16).[67]

The ADPPA incorporated express preemption of current state data privacy laws but carved out and excluded the Biometric Information Privacy Act, the Genetic Information Privacy Act, and the CCPA/CPRA from preemption.[68] These acts are state data privacy laws passed in California and Illinois.[69] In the next part of this Note, these pieces of legislation will be expanded upon. But for now, it is important to consider how this express preemption exclusion interplays with changing state laws. If these laws were to be amended in the future, would the amendments have continued to be considered a carve-out?

Under the previously proposed ADPPA, "[b]eginning [two] years after the ADPPA's effective date, the bill provides a private right of action for consumers alleging violations.[70] This [delayed] private right of action is subject to certain procedural requirements."[71] The individual must notify the FTC and the state Attorney General in writing for their civil claim.[72] The FTC and the state Attorney General have 60 days to respond as to whether they will seek action.[73] If they take action, the prospective plaintiff cannot pursue their private claim.[74] However, some prospective defendants have a forty-five day right to cure the alleged violation.[75] Remedies for a violation of the ADPPA include an amount equal to the sum of any compensatory damages,

---

67. *Id.*

68. *Id.*

69. *Id; see also* 740 ICLS 14 et seq; 410 ILCS 513 et seq; Section 1798.150 of the California Civil Code (as amended on November 3, 2020 by initiative Proposition 24, Section 16).

70. *American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?*, BASS, BERRY & SIMS PLC (June 21, 2022); *see also* H.R. 8152.

71. *See American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?,*
supra note 70.

72. Lucas Schaetzel, *Proposed Federal Data Protection Law Would Impose Duty of Loyalty and Allow Limited Private Right of Action*, BENESCH (July 6, 2022), https://www.jdsupra.com/legalnews/proposed-federal-data-protection-law-2203514/.

73. *Id*.

74. *Id*.

75. *See American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?*, *supra* note 70; *see also* H.R. 8152.

injunctive relief, declaratory relief, and reasonable attorneys' fees and litigation costs.[76] Additionally, some violations may be considered unfair or deceptive under the FTC Act, including penalties up to $10,000 per violation.[77] The private right of action section does not apply to any covered entities that have less than $25,000,000 per year in revenue; collects, processes, or transfers the covered data of fewer than 50,000 individuals; or derives less than fifty percent of its revenue from transferring covered data.[78]

D. Critiques & Recommendations

It is difficult to weigh the impact and consequences of the laws and regulations set forth in the ADPPA. On one hand, it is important to have a uniform data protection act that is consistent throughout the entire United States. With this consistency, it is easier for both companies and consumers to understand the rights afforded to consumers so companies can instill policies and procedures to support these rights. With the current state framework, companies must navigate a minefield of state laws and try to abide by the individual laws where business operations are conducted in each respective state. The main goal is to protect the consumers, so a clear and uniform understanding of the law is important to adequately provide meaningful data privacy protection to consumers. Moreover, it is important to protect the residents of the states that have fewer data privacy protection laws because some states have unequal data protection regulations compared to their sister states.[79] The ADPPA aimed to cure this imbalance by providing uniformity and to protect all states under this piece of sweeping legislation.

On the other hand, technology moves at a quick pace. Congress enacting federal legislation has been known to historically move at a slower pace than states enacting legislation.[80] The juxtaposition of rapid changing technology and a slow-moving legislative process could become problematic in the future. The ADPPA would need to

76. *See American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?*, *supra* note 70; *see also* H.R. 8152.

77. *See American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?*, *supra* note 70.

78. *See* H.R. 8152.

79. *See 47 States Have Weak or Nonexistent Consumer Data Privacy Laws*, *supra* note 11.

80. *State Legislatures Vs. Congress: Which Is More Productive*?, QUORUM, https://www.quorum.us/data-driven-insights/state-legislatures-versus-congress-which-is-more-productive (last visited Sept. 24, 2023).

evolve with the technology and circumstances by adapting through its own provisions.[81] If Congress does not adapt to technology changes quickly, there lies the issue of preemption. States would be preempted from evolving the law to match the improving technology even though Congress could remain silent on these future issues. This leaves the average consumer at a loss for data protection and can potentially strip an individual's rights. State Senator Reuven Carlyle, (D-Wash.) said, "I do have a sensitivity to a patchwork between states. But Congress can't have it both ways where it sets a low floor and then prohibits states from innovating."[82]

To solve and balance these issues, one idea would be for Congress to set a minimum threshold, with states having the ability to create stricter standards. This circumvents the problem regarding the shifting technological landscape coupled with Congress' potential inability to keep up while offering protection to consumers in all fifty states. Additionally, it helps companies navigate the current minefield of state data privacy laws by having more uniformity in decision-making and policy creation throughout the entire United States. This change would also please the states, such as California, that would prefer stricter and more detailed laws for its residents and would allow it to enact state legislation doing so.

Furthermore, the private right of action is another hot topic previously proposed in the ADPPA. Some critics feel the ADPPA did not provide a lucrative private right of action.[83] These critics claim the two-year delay in being able to bring claims was too long.[84] Critics say people should be able to bring claims immediately because two years is a significant amount of time for companies to have abusive data practices while consumers are not able to recover any damages.[85] Moreover, the scope of the private right of action was not as encompassing as many critics would have preferred.[86] For example, the bill denied private litigation for many of the bill's core protections,

81. Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, INT'L ASS'N OF PRIV. PROS. (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus.

82. *Id*.

83. Hayley Tsukayama, et al., *Americans Deserve More Than the Current American Data Privacy Protection*, EFF: DEEPLINKS BLOG (July 24, 2022), https://www.eff.org/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act.

84. Tsukayama, *supra* note 83; *see also* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

85. Tsukayama, *supra* note 83.

86. *Id.*

including data minimization, algorithmic transparency, and unified opt-out mechanisms.[87] Senator Maria Cantwell (D-Wash.) said, "she couldn't support the bipartisan framework unless House lawmakers add tougher enforcement measures, including limits on forced arbitration and a broad right for individuals to sue companies that violate the law."[88] Critics claim the bill should also have included liquidated damages, punitive damages, as well as abolishing the procedural hurdles before a suit can go forward.[89]

On the flip side, the private right of action may have opened the flood gates for litigation and clogged the courts' dockets. Adam Kovacevich, the CEO of Chamber of Progress, said, "I don't think anyone in [the] industry is crazy about the idea of the private right of action, the idea of more lawsuits."[90] Since a potential reward under the ADPPA was attorneys' fees, there was an incentive for plaintiffs' attorneys to generate new cases.[91] Neil Bradley, U.S. Chamber of Commerce Executive Vice President and Chief Policy Officer, said:

> More than 130 countries have enacted general privacy protections, and five state legislatures have passed comprehensive data protection bills. However, for good reason, private right of action for privacy is not included in any of these states' laws, nor is it part of the European Union's General Data Protection Regulation.[92]

Even though a private right of action can reward the person who was harmed, the system may be abused to harass companies and competition, or to seek awards and monetary damages when there may not be merit for a claim. One way to help solve this problem could be to expand and increase the period to cure. If companies received an increased period to rectify the error or breach, then this may limit potentially frivolous claims. With many disagreements and conflictions

87. *Id.*

88. David Stauss & Shelby Dolen, *Analyzing the American Data Privacy and Protection Act's Private Right of Action,* HUSCH BLACKWELL (Aug. 1, 2022), https://www.bytebacklaw.com/2022/08/analyzing-the-american-data-privacy-and-protection-acts-private-right-of-action.

89. Tsukayama, *supra* note 83; *see also* H.R. 8152.

90. Gilad Edelman, *Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill*, WIRED (July 21, 2022, 8:08 AM), https://www.wired.com/story/american-data-privacy-protection-act-adppa.

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

92. *Id.*

surrounding the previously proposed ADPPA, New York should seek to enact the New York Privacy Act S365, with some revisions, regardless of potential federal legislation on the horizon because New Yorkers should be afforded proper personal data privacy protection while giving companies clear and comprehensive guidelines.

III. STATE LAWS: CALIFORNIA & ILLINOIS

Congress has been silent on successfully passing a sweeping and overarching consumer data privacy regulation in the United States. As a result, state legislators have taken matters into their own hands and have been passing state specific laws to give their residents a right to data privacy protection. Specifically, the most notable legislation that has been passed in recent years has been from California and Illinois.[93]

A. California: CCPA & CPRA

California was the first state to lead the charge in state enacted data privacy protection.[94] On June 28, 2018, Governor Jerry Brown (D-Calif.), signed the California Consumer Privacy Act (CCPA) into law.[95] The CCPA took effect January 1, 2020.[96] The CCPA offers data privacy rights to consumers by creating standards and obligations for businesses to abide by when collecting and selling personal information.[97] Specifically, it protects California residents from harmful data practices by companies doing business in California.[98] However, to be regulated by the CCPA, these companies need to fall into one of three categories:

> A company must either (1) have annual gross revenues of more than $25 million; (2) buy, receive, sell, or share the personal information of more than 50,000 consumers, households, or

93. *See generally* California Consumer Privacy Act of 2018, CAL. CIVIL § 1798.100 (West 2023), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100 (last visited Sept. 22, 2023); Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (providing details of California and Illinois data privacy legislation).

94. *Which States Have Consumer Data Privacy Laws?,* BL, https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/ (last visited Oct. 1, 2023).

95. *CCPA and CPRA* Topic Page, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/topics/ccpa-and-cpra (last visited Sept. 22, 2023).

96. *California Consumer Privacy Laws*, BL, https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/ (last visited Sept. 22, 2023).

97. *Id.*

98. Cook, *supra* note 15, at 776.

> devices (either in one category or across all categories); or (3) derive at least 50% of its annual revenues from sales of consumers' personal information.[99]

With these guidelines on which companies are regulated, there are two important notes. First, the CCPA only protects California residents, which can include a resident who is temporarily outside the state.[100] Second, the CCPA does not apply to not-for-profit or government entities.[101] Thus, the protected consumer and the regulated company are both limited in scope compared to the GDPR.[102]

The privacy rights offered to California residents includes the right to know about the personal information a business collects about them, how it is used, and how it is shared; the right to delete personal information collected from them; the right to opt out of the sale of their personal information; and the right to non-discrimination for exercising their CCPA rights.[103] The CCPA defines personal information as information that identifies, relates to, or could reasonably be linked with you or your household.[104] Examples of personal information would be name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.[105]

For most violations under the CCPA, the Attorney General or the California Privacy Protection Agency can file an action against the business.[106] The Attorney General does not represent individual California consumers.[107] "Using consumer complaints and other information, the Attorney General may identify patterns of misconduct that may lead to investigations and actions on behalf of the collective legal interests of the people of California."[108] If there is a data breach:

> [A consumer] can sue a business if your nonencrypted and nonredacted personal information was stolen. . .as a result of the business's failure to maintain reasonable security

---

99. *Id.*

100. *California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (last visited Sept. 22, 2023).

101. Cook, *supra* note 15, at 776.

102. *Id.*

103. *California Consumer Privacy Act (CCPA)*, *supra* note 100.

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

108. *California Consumer Privacy Act (CCPA)*, *supra* note 100.

> procedures and practices to protect it. If this happens, you can sue for the amount of monetary damages you actually suffered from the breach or "statutory damages" of up to $750 per incident.[109]

It is important to note the CCPA's enforcement of violations is far different from the ADPPA's private right of action. The CCPA has little to no private right of action, with minimal rewards.[110]

The California Privacy Rights Act (CPRA), also known as Proposition 24, is a ballot measure that was approved by California voters on November 3, 2020.[111] It significantly amends and expands the CCPA, and it is sometimes referred to as "CCPA 2.0."[112] The CPRA took effect on December 16, 2020, with most provisions becoming operative on January 1, 2023.[113] The CPRA offers many notable amendments to the CCPA. First, the CPRA establishes the California Privacy Protection Agency.[114] This newly established agency is "vested with 'full administrative power, authority, and jurisdiction to implement and enforce' the CCPA."[115] However, this does not take away from the Attorney General's enforcement powers given under the CCPA.[116] Second, the CPRA gives two additional rights to consumers.[117] Consumers have the right to correct inaccurate personal information, and the right to limit the use and disclosure of sensitive personal information.[118] Finally, the CPRA expands upon personal information and creates "sensitive personal information."[119] Sensitive personal information was inspired by special categories of personal data in the GDPR.[120] The CPRA defines "sensitive personal information" as:

> [P]ersonal information that reveals: a consumer's social security number or other state identification number; a consumer's account log-in information, financial account details, debit

109. *Id*.

110. *See* California Consumer Privacy Act of 2018, CAL. CIVIL § 1798.100 (West 2023).

111. *California Consumer Privacy Law*, *supra* note 96.

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.*

116. *California Consumer Privacy Law*, *supra* note 96.

117. *Id.*

118. *Id.*

119. *Id.*

120. *How do CPRA treat sensitive personal information,* SECURITI (Aug. 25, 2022), https://securiti.ai/blog/cpra-sensitive-personal-informations.

> card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's geolocation; a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; the contents of a consumer's mail, email, or text messages, unless the business is the intended recipient of the communication; and a consumer's genetic data.[121]

The CCPA and CPRA are landmark pieces of consumer data privacy legislation and the drafters of the ADPPA sought to include a carve-out for these laws to remain in effect. Another important carve-out offered in the ADPPA was Illinois' Biometric Information Privacy Act.[122]

B. Illinois: Biometric Information Privacy Act

Illinois' Biometric Information Privacy Act (BIPA) is not necessarily a sweeping piece of data privacy regulation, but rather an important piece of legislation companies should be aware of due to its impact on business and its once potential carve-out in the ADPPA.

> [The] BIPA requires entities, including employers, that collect biometric data to follow a number of protocols, including maintaining a written policy about the collection and storage of biometric data, providing owners of biometric information with written notice of such practices, and obtaining informed consent from individuals subject to biometric data collection.[123]

Companies should be aware of BIPA because the Illinois Supreme Court often favors plaintiffs in BIPA cases.[124] Though only impactful for companies doing business in Illinois, other states may enact their own biometric information laws so companies should keep an eye out for legislation related to the states they conduct business in.

---

121. *Handling Sensitive Personal Information Under the CPRA and the VCDPA,* CLARIP, https://www.clarip.com/data-privacy/handling-sensitive-personal-information-under-the-cpra-and-the-vcdpa **(**last visited Sept. 19, 2023).

122. *See* American Data Privacy and Protection Act, H.R. 8152 § 404, 117th Cong. (2022).

123. Adam S. Forman & Nathaniel M. Glasser, *Employers Take Heed: Follow Illinois Biometric Privacy Rules or Risk a Losing Battle*, NAT'L L. REV. (Feb. 16, 2022), https://www.natlawreview.com/article/employers-take-heed-follow-illinois-biometric-privacy-rules-or-risk-losing-battle; *See also* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

124. Forman & Glasser, *supra* note 123; 740 ILCS 14/5.

IV. NEW YORK PRIVACY ACT – S365

Introduced on January 4, 2023, by Senators Thomas, Comrie, Jackson, Krueger, May, and Ramos, the New York Privacy Act (NYPA) seeks to offer New York residents consumer data privacy protection.[125] As of February 26, 2023, the NYPA has been introduced to the Senate and referred to the Consumer Protection Committee.[126]

A. New York Privacy Act – Who?

To be regulated by the NYPA, a company needs to conduct business in the state of New York or have products or services targeted at New York residents.[127] Furthermore, to be regulated by the NYPA, a company must fall into one or more of the following categories: the company has an annual gross revenue of at least $25,000,000; the company controls or processes the personal data of at least 100,000 New York consumers; the company controls or processes the personal data of at least 500,000 people nationwide and controls or processes personal data of at least 10,000 New York consumers; or the company derives over fifty percent of gross revenue from the sale of personal data and controls or processes personal data of at least 25,000 New York consumers.[128] It is important to note the NYPA mainly protects New York residents, similar to how the CCPA mainly protects California residents.[129]

B. New York Privacy Act – Scope, Enforcement, & Remedies

There are a few key provisions in the NYPA offering rights to consumers which may impact a regulated company's business operations. First, the NYPA establishes the right to confirm whether a business is processing a consumer's personal information and the right to access the personal information; the right to correct inaccuracies in the consumer's personal information; the right to delete personal data about the consumer; the right to obtain a copy of the data in a portable and readily usable format; and the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or

125. N.Y. Privacy Act, S.B.365, 2023–24 Leg., 246th Sess. (N.Y. 2023).

126. *Id.*

127. *Id.*

128. S.B.365; *e.g.,* Kirk J. Nahra, et al., *State Comprehensive Privacy Law Update for 2023*, WILMER CUTLER PICKERING HALE AND DORR (Jan. 19, 2023), https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20230119-state-comprehensive-privacy-law-update-for-2023.

129. *See* S.B.365.

similarly significant effects concerning the consumer.[130] Second, consent is required to process a consumer's personal data, and consent is also required to make changes to existing processing purposes that may result in less protection which a consumer has already consented.[131] Third, the NYPA incorporates privacy by design principles, such as a purpose limitation and reasonable safeguards to protect consumer data.[132] Fourth, the NYPA requires data brokers to register, pay an annual fee to the New York Attorney General, and submit information regarding their data usage practices including a description of the method of processing consumer requests.[133] Finally, the NYPA creates a private right of action to recover actual damages suffered and reasonable attorneys' fees.[134] Notwithstanding the private right of action, the New York Attorney General can bring action to enjoin any violation, to obtain restitution and disgorgement of any money or property obtained by the violation, and to obtain civil penalties of up to $15,000 per violation.[135] If passed, the NYPA will take effect immediately, with some sections taking effect two years after enactment, and the private right of action taking effect three years after enactment.[136]

C. Revise & Enact the NYPA

The NYPA offers New Yorkers data privacy rights and gives clear instructions to companies on how to navigate these rights. Because of its clarity, the NYPA should be enacted regardless of a potential federal preemption of this bill. The ADPPA is not certain to be passed. In fact, there has been no success in recent history passing federal legislation offering broad data privacy protection to the citizens of the United States. First, in March 2021, Representative Suzan DelBene (D-WA) introduced the Information Transparency and Personal Data Control Act which has not been acted on since.[137] Second, in May 2021, Senators John Kennedy (R-LA) and Amy Klobuchar (D-MN) introduced the bipartisan Social Media Privacy Protection and Consumer Rights Act which has not been acted on since.[138] Finally, in

130. *Id.*
131. *Id.*
132. S.B.365; *e.g.,* Nahra, et al., *supra* note 128.
133. S.B.365.
134. *Id.*
135. *Id.*
136. *Id.*
137. Cook, *supra* note 15, at 772–73.
138. *Id.* at 773.

July 2021, Senators Roger Wicker (R-MS) and Marsha Blackburn (R-TN) introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act which has not been acted on since.[139] All three of these proposed acts were overarching pieces of federal legislation focused on consumer data privacy protection. All three of these acts did not receive any traction. If previous bills did not make any progress, the ADPPA will likely have a similar fate. Without the ADPPA, it is up to New York legislators to enact the NYPA to offer data privacy protection to its citizens.

Although the NYPA should be enacted, there should be certain revisions to the bill. New York legislatures should reconsider the private right of action clause. California's CCPA, the forefront of state consumer data privacy laws, has a much narrower authority for a private right of action than the proposed NYPA.[140] Even the CPRA, after real world application of the CCPA, did not include a private right of action as broadly proposed in the NYPA.[141] The NYPA's private right of action is far too inclusive allowing private citizens to bring suit for most of the proposed consumer protections. The proposed bill's private right of action is not only just broad, but awards attorneys' fees to the prevailing plaintiffs.[142] If the court has discretion to award attorneys' fees, that can be an incentive for plaintiffs to bring meritless claims. This could result in frivolous lawsuits clogging the already busy docket of the New York State court system. Moreover, some people could abuse this private right of action to bother competitors by making them spend time and money on warrantless litigation.

However, the private right of action can be helpful for the citizens of New York who were harmed by abusive company practices and suffered real life consequences. It can be argued the three-year rollover period soothes the transition and is helpful for companies to instill the necessary practices without being bombarded by litigation. While this period may help ease the negative externalities associated with the private right of action, the negative externalities may impose a greater burden than benefit on the courts and the companies trying to run a sound business.

---

139. *Id.* at 774.

140. *New York Privacy Act Update: Bill Out of Committee, Moves to Full Senate*, GIBSON, DUNN & CRUTCHER (May 21, 2021), https://www.gibsondunn.com/new-york-privacy-act-update-bill-out-of-committee-moves-to-full-senate.

141. *See id.*

142. N.Y. Privacy Act, S.B.365, 2023–24 Leg., 246th Sess. (N.Y. 2023).

To balance these two opposing arguments, a potential revision to the NYPA is to instill a cure period allowing for a company to correct an alleged violation. For example, the ADPPA offered some prospective defendants a forty-five day right to cure period for an alleged violation.[143] By affording companies a window to cure, this may help reduce potential litigation because companies can rectify any potential breaches, claims, or insecurities the consumer may have about the companies' practices. The window of time will essentially act as a buffer for the plaintiff, defendant, and the court to comprehend the claim and determine its merit. With these slight tweaks, it is imperative New York legislators pass the NYPA because an overarching federal consumer data privacy bill is not certain. New York should seek to enact the New York Privacy Act S365, with some revisions, regardless of potential federal legislation on the horizon because New Yorkers should be afforded proper personal data privacy protection while giving companies clear and comprehensive guidelines.

CONCLUSION

Ultimately, protecting consumers and giving clear guidance to companies should be the legislators' main goal. In the coming years, the legal landscape will continue to morph as technological innovations progress. Staying on top of the curve is critical, especially for such an innovative state as New York. New York should seek to enact the New York Privacy Act S365, with some revisions, regardless of potential federal legislation on the horizon because New Yorkers should be afforded proper personal data privacy protection while giving companies clear and comprehensive guidelines.

143. *American Data Privacy and Protection Act – Could a Federal Privacy Law be on the Horizon?,*
supra note 70; *see also* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 403(c)(2) (2022).