Volume 125 | Issue 1 Article 9

September 2022

What a Data Privacy Law Should Look Like in West Virginia: Balancing Competing Interests of Consumers and Businesses

Harrison Enright
West Virginia University College of Law

WHAT A DATA PRIVACY LAW SHOULD LOOK LIKE IN WEST VIRGINIA: BALANCING COMPETING INTERESTS OF CONSUMERS AND BUSINESSES

ABSTRACT

Today's businesses invariably leverage consumer data to create business insights, such as marketing strategies and consumer behavior analyses. As a result, consumers have placed an emphasis on data privacy and security. In response, many states have proposed comprehensive legislation aspiring to regulate the collection and usage of consumer data by businesses, grant individual rights to consumers, and provide for a method of enforcement. House Bill 3159 represents West Virginia's most recent attempt at doing so, serving as an indication that the state is working diligently to enhance the data privacy of its residents.

Although enacting a comprehensive data privacy law in West Virginia would symbolize an important victory for consumers, such a law would simultaneously carry a risk of inhibiting business growth by restricting the availability of consumer data. Accordingly, the state legislature must prioritize striking a balance between the competing interests of consumers and businesses. To do so, the law must offer sufficient protection for consumer data without unduly hindering business innovation using that data.

After surveying analogous laws in other states, this Note argues for the inclusion of several features within a data privacy law in West Virginia to achieve that balance: (1) a distinction between ordinary and sensitive consumer data; (2) a right to opt-out of certain processing activities; (3) an applicability framework that requires compliance only from businesses that collect and/or use a substantial amount of consumer data; (4) a duty to practice data minimization and to conduct data protection assessments; and (5) private right of action qualified by a cure period for businesses.

TABLE OF CONTENTS

I. INTRODUCTION TO THE U.S. DATA PRIVACY LANDSCAPE

> *[P]rotecting . . . citizens' data privacy from potentially data-abusing corporations . . . will have consequences equally as threatening to a nation's global stance in this race to innovate as exposure does to individuals' privacy interests. The real battle will be treading the line between protecting citizens' privacy and facilitating technological growth.*[1]

In modern society, "[d]ata is the engine that is driving commerce around the world."[2] Given the emergence of the Internet of Things,[3] the advancement of machine learning algorithms,[4] and the rise of data brokers,[5] data now fulfills an unprecedented function in the U.S. economy. A vast majority of modern businesses leverage consumer data to create business insights, such as for purposes of targeted advertising and the creation of customer profiles.[6] In recent decades, this practice has become critical to remaining competitive in many industries.[7]

Growing consumer concerns over the protection and security of consumer data have accompanied this development.[8] These concerns range from

---

1 Sydney Wolofsky, *What's Your Privacy Worth on the Global Tech Market? Weighing the Cost of Protecting Consumer Data Against the Risk That New Legislation May Stifle Competition and Innovation During This Global, Technological Revolution*, 44 FORDHAM INT'L L.J. 1149, 1153 (Apr. 2021).

2 *See* Kirk J. Nahra, *The Past, Present, and Future of U.S. Privacy Law*, 51 SETON HALL L. REV. 1549, 1563 (2021).

3 *See id.* ("The Internet of Things is leading a wide range of industries to now view data gathering and analytics as a primary mode of behavior.").

4 *See* Jena Martin, *Data Privacy Issues in West Virginia: An Overview*, 124 W. VA. L. REV. ONLINE 1, 3 (2021) (noting that "data that once required thousands of hours to organize, collate, and sort, can now all be managed with the press of the button that often activates a machine-learning algorithm.").

5 *See id.* (noting that, while often invisible to the public eye, data brokers are important entities in the collection and processing of consumer data).

6 *See* Nahra, *supra* note 2, at 1561.

7 *See* Diane Y. Byun, *Privacy or Protection: The Catch-22 of the CCPA*, 32 LOY. CONSUMER L. REV. 246, 264–65 (2020) ("[w]ithout the ability to track consumer responses or predict consumer expectations, it is nigh on impossible for a small business to compete with incumbents like Google or Facebook.").

8 *See* Brooke Auxier, *How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak*, PEW RSCH. CTR. (May 4, 2020), https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ ("Roughly eight-in-ten adults (79%) said they were at least somewhat concerned about how companies were using the data collected about them . . . . Yet relatively few Americans said they

the frequency of data breaches to the potential of algorithms to have a discriminatory impact on consumers.[9] Eventually, consumers began to lobby for legal protections to alleviate these fears. In response, Congress first created sectoral laws to establish federal baselines for protection, including the Gramm-Leach-Bliley Act (financial services) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) (medical services).[10] A later wave of legislation increasingly focused on regulating certain practices involving personal data, such as the Children's Online Privacy Protection Act (COPPA) and Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM).[11] Related developments at the state level have included laws governing data breach notification and data security.[12]

Notwithstanding these legal developments, however, the continued progression of data analytics into nearly all commercial contexts left consumers with more doubts than protection.[13] As a result, proposals for more extensive protection began to gain traction, leading to the advent of comprehensive data privacy laws.[14] And without a federal law on the horizon, state legislatures have aspired to employ data privacy legislation[15] at the state level to counter the power imbalance that currently exists between consumers and businesses.[16] However,

understood a great deal what was being done with the data collected about them by companies (6%).").

9 *See* Martin, *supra* note 4, at 10 (identifying focus group recommendations to include restrictions on retention of consumer data by businesses and a ban on prejudicial targeted advertising); Tabrez Y. Ebrahim, *Algorithms in Business, Merchant-Consumer Interactions, & Regulation*, 123 W. VA. L. REV. 873, 899 (2021) (noting that "[d]ifferences in jurisdictions' approaches include protecting consumers against information asymmetry, power imbalances, and discrimination and striving to achieve transparency and accountability, privacy, and non-discrimination").

10 *See* Nahra, *supra* note 2, at 1551.

11 *Id.* at 1552–53.

12 Camila Tobón, *U.S. State Privacy and Data Security Laws: An Overview*, ROCKY MOUNTAIN MIN. L. FOUND. SPECIAL INST. *8-1 (Apr. 7, 2021).

13 *See* Auxier, *supra* note 8 ("Six-in-ten Americans (63%) said in 2019 that they knew very little or nothing at all about the laws and regulations currently in place to protect their data privacy . . . . However, three-quarters of Americans said they thought there should be more government regulation of what companies can do with their customers' personal information. . . .").

14 Nahra, *supra* note 2, at 1553.

15 *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022); California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301–1313 (West 2022); Virginia Consumer Data Protection Act, VA. CODE §§ 59.1-575–59.1-585 (West 2022).

16 *See* Ebrahim, *supra* note 9, at 874 (arguing that "countervailing consumer empowerment is necessary to balance the power between merchants and consumers"); Alexander R. Migliorini, *The Big Box Versus the Mom & Pop Shop: The Beauty of the (Data Privacy) Bills Are in the Eye of the Beholder*, 19 J. INT'L BUS. & L. 232, 257 (2020) (arguing that "Americans will undoubtedly gain

the overwhelming majority of states have yet to succeed in passing such legislation, including West Virginia.

House Bill 3159 represents West Virginia's most recent attempt at enhancing the data privacy of its residents.[17] Although House Bill 3159 failed to become law, West Virginia would be well-advised to follow California,[18] Virginia,[19] and Colorado[20] by enacting a comprehensive data privacy law. A desire to mitigate risks associated with business collection and retention of consumer data remains prevalent in West Virginia: in a recent survey of 500 West Virginia residents,[21] "responses demonstrated that many residents in West Virginia would like to see some specific remedy for data privacy harm."[22]

This Note argues for the inclusion of several features within a comprehensive data privacy law in West Virginia. Each of these features would further the policy that should be adhered to in drafting any data privacy legislation: offering meaningful protection for consumer data without unnecessarily hindering business innovation through the collection and use of that data.

First, a data privacy law in West Virginia should distinguish between ordinary and sensitive consumer data, offering consumers a right to limit businesses from processing their sensitive data. Second, the law should limit the consumer's right to opt-out to a well-defined set of processing activities, such as for sales, targeted advertising, and profiling. Third, the law should only require compliance from businesses that either (1) process the personal information of at least 100,000 consumers or (2) derive a substantial percentage of their revenue from selling consumer data. Accordingly, the law should exclude a CCPA-like annual gross revenue threshold. Fourth, the law should place businesses under a duty to practice data minimization and to conduct data protection assessments for processing activities carrying a heightened risk of consumer harm, such as for sales, targeted advertising, and profiling. Fifth, the law should authorize a limited private right of action for consumers, subject to a grace period for businesses to cure violations.

Following this introduction, this Note proceeds in four parts. Part II surveys developments in the U.S. data privacy landscape to explore legislative

---

leverage over large businesses hungry for organic data, establishing a market for consumers to profit from their data and conferring a pecuniary power to the public" through data privacy laws.).

17 H.B. 3159, 85th Leg., 2d. Sess. (W. Va. 2021).

18 *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022); California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022).

19 *See* Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2022).

20 *See* COLO. REV. STAT. §§ 6-1-1301–1313 (West 2022).

21 *See* Martin, *supra* note 4, at 8.

22 *Id.*

trends derived from recent data privacy legislation. Part III conducts a similar analysis of W. Va. House Bill 3159 in search of flaws that may have presented an obstacle to passage. In light of the shortcomings identified in Part III, Part IV recommends the inclusion of several features within a future data privacy bill in West Virginia. These recommendations aspire to alleviate concerns that may have precluded House Bill 3159 from becoming law and to strike a balance between competing interests. Part V concludes by offering policy justifications and reviewing how such a law would fit into the current U.S. data privacy landscape.

II. EMERGING TRENDS FROM THE EVOLUTION OF U.S. DATA PRIVACY LAW

Throughout the evolution of U.S. data privacy, state legislatures have increasingly sought to regulate the collection and usage of consumer data through comprehensive data privacy laws. A few states have already proved successful in these efforts; namely, California, Virginia, and Colorado have each passed comprehensive data privacy laws.[23] However, the fate of pending data privacy legislation in a number of other states remains to be seen,[24] and still, other states continue to revise data privacy bills that ultimately failed to become law.[25]

Several trends have emerged from this abundance of data privacy legislation. The most pertinent of these trends concern the scope of protection, consumer rights, applicability to businesses, business obligations, and enforcement mechanisms embodied in these laws. Appreciation of these trends carries importance in forecasting what an analogous law should resemble once inevitably passed in West Virginia. This section explores these legislative tendencies and discusses important differences between data privacy laws across the country. This investigation focuses on five important facets of these laws: (1) scope of protection, (2) consumer rights, (3) applicability to businesses, (4) business obligations, and (5) enforcement mechanism.

---

[23] *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022); California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301–1313 (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2022).

[24] *See, e.g.*, H.B. 1492, 92d Leg., Reg. Sess. (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021).

[25] *See, e.g.*, H.B. 216, 2021 Gen. Assemb., Reg. Sess. (Ala. 2021); H.B. 969, 2021 Gen. Assemb., Reg. Sess. (Fla. 2021); H.B. 3741, 87th Leg., Reg. Sess. (Tex. 2021); S.B. 5062, 2021 Gen. Assemb., Reg. Sess. (Wash. 2021); H.D. 3159, 85th Leg., Reg. Sess. (W. Va. 2021).

A. The California Consumer Privacy Act of 2018 ("CCPA") & California Privacy Rights Act of 2020 ("CPRA")

California was the first state to enact a comprehensive data privacy law. Viewed as a "groundbreaking" step in U.S. privacy law,[26] the California Consumer Privacy Act of 2018 ("CCPA")[27] created an "all-purpose" framework for the protection of consumer data.[28] Just two years later, the state passed the California Privacy Rights Act of 2020 ("CPRA")[29] to amend certain aspects of the CCPA. The template established by these laws has since become a foundation for safeguarding consumer data, which other states have integrated into their own data privacy laws.

1. Scope of Protection

Among the "groundbreaking" characteristics of the CCPA is the law's noticeably broad definition of "personal information."[30] Under the CCPA, "personal information" is defined to include personal identifiers, characteristics of protected classifications, commercial information, biometric information, internet activity information, geolocation data, certain employment information, non-public educational information, and inferences drawn from the aforementioned information to create a consumer profile.[31] "With its broad definitions of covered individuals, entities, data categories, and practices, the CCPA casts a wide net in an effort to protect [c]onsumers through increased data privacy."[32] In doing so, the California state legislature almost certainly intended to "future proof" the law's application as the collection and usage of consumer data by businesses continues to evolve with technological advancements.[33]

---

26 Nahra, *supra* note 2, at 1553.

27 California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022).

28 Nahra, *supra* note 2, at 1553.

29 California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022).

30 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(v)(1) (West 2022) (defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

31 *See generally id.* § 1798.140.

32 Byun, *supra* note 7, at 248.

33 Nahra, *supra* note 2, at 1561.

On the other hand, the CCPA is not applicable to certain medical[34] and financial[35] information or to consumer data that is publicly available.[36] The CCPA also exempts nonprofit organizations and government agencies.[37] Thus, although the CCPA generally "casts a wide net" in its quest to protect consumer data,[38] a number of exceptions fine-tune the scope of this protection.

Despite its emphasis on providing security for consumer data, the original CCPA did not distinguish between "personal information" and what more recent legislation has coined "sensitive" consumer data.[39] The CCPA initially treated all consumer data as equal under the law, regardless of its nature. After further deliberation, however, the state legislature included such a distinction in the CPRA.[40] Under the CPRA, "sensitive personal information" is defined to include consumer data revealing a consumer's social security, driver's license, state identification card, or passport number; financial account information; precise geolocation; race; ethnicity; religion; health; biometrics; and private communications (content of emails and text messages).[41]

The importance of this distinction lies in the additional protection afforded to "sensitive personal information."[42] The CPRA grants consumers "the right . . . to direct a business . . . to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer."[43] As a result, consumers receive greater control over how businesses use their most delicate personal information.

---

34 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.145(c)(1)(A) (West 2022) (excluding "[m]edical information governed by the Confidentiality of Medical Information Act" as well as "protected health information that is collected by a covered entity . . . governed by the privacy, security, and breach notification rules [established pursuant to HIPAA]").

35 *Id.* § 1798.145(e) (excluding "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act.").

36 *Id*. § 1798.140(v)(2) (defining "publicly available" as "information that is lawfully made available from federal, state, or local government records").

37 *California Consumer Privacy Act*, STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Sept. 6, 2022).

38 Byun, *supra* note 7, at 248.

39 *See, e.g.*, Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303 (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 (West 2022).

40 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.140(o) (West 2022).

41 *Id.*

42 *Id.* § 1798.121.

43 *Id.*

2. Consumer Rights

A second "groundbreaking" feature of the CCPA is the bundle of rights it grants to consumers over their personal information following collection. These include (1) a right to request access to their personal information as collected or sold by businesses,[44] (2) a right to direct businesses to delete their personal information,[45] and (3) a right to opt-out of the sale of their personal information to third parties.[46] Additionally, the CCPA grants consumers a right against discrimination in the price and quality of products offered by a business if the consumer chooses to exercise these rights under the law.[47]

The CPRA expands on the original right to opt-out under the CCPA by enabling consumers to opt-out of the "sharing"[48] of their personal information with third parties.[49] Moreover, the CPRA adds a consumer right to direct businesses to use "commercially reasonable" efforts to correct inaccurate personal information.[50] By granting these rights, the CCPA and CPRA promote active participation by consumers in safeguarding their data, a recurring theme throughout the U.S. data privacy landscape.

3. Applicability

A third "groundbreaking" aspect of the CCPA relates to its applicability to businesses. The CCPA limits its definition of "business" to entities that operate for profit, conduct business within the state, and collect and/or use personal information.[51] Further, compliance is only required from those businesses that meet one or more of the following thresholds: (1) generates at least $25,000,000 in annual gross revenue; (2) annually buys or sells the personal information of at least 50,000 consumers; or (3) derives at least 50% of their annual gross revenue

---

44 California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.110, 1798.115 (West 2022).

45 *Id.* § 1798.105.

46 *Id.* § 1798.120.

47 *Id.* § 1798.125.

48 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.140(ah)(1) (West 2022) (defining "sharing" as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration").

49 *Id.* § 1798.120 ("A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information.").

50 *Id.* § 1798.106 ("A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information . . . .").

51 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(d) (West 2022).

from the sale of personal information.[52] The CPRA increases this second threshold to businesses that process the personal information of at least 100,000 consumers[53] and adds the "sharing" of personal information with third parties to the calculation of both the second and third thresholds.[54]

Although the ultimate effect of these threshold limitations has been disputed,[55] they were likely intended to exempt small businesses that only commercialize a negligible amount of consumer data from compliance. Regardless, these threshold limitations to applicability continue to curtail the "wide net"[56] cast by the CCPA's sweeping definition of "personal information."

4. Enforcement

Importantly, a fourth "groundbreaking" characteristic of the CCPA is the limited private right of action it confers upon consumers.[57] Under the law, consumers whose personal information is subject to unauthorized access or disclosure due to the failure of a business "to implement and maintain reasonable security procedures" may initiate a civil action against the business if the violation is not cured within a 30-day grace period.[58] Consumers may seek monetary damages as well as injunctive and declaratory relief in these actions.[59] This private right of action again encourages active participation by consumers in the protection of their consumer data.

The CPRA expands on the original private right of action by including consumers "whose email address in combination with a password or security question and answer that would permit access to the account" is subject to a breach.[60] In doing so, the CPRA broadens the circumstances under which

---

52 *Id.*

53 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.140(c) (West 2022).

54 *Id.* § 1798.140(d)(1)(B).

55 *Compare* Byun, *supra* note 7, at 249 (arguing that the CCPA's "low threshold [encompasses] more than just the data giants that inspired this stringent law. Consequently, businesses with limited resources ('small businesses') are further disadvantaged in the marketplace due to costs associated with compliance.") *with* Katherine M. Wilcox, *"Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation*, 85 BROOK. L. REV. 257, 280 (2019) ("[T]he CCPA includes a carve-out exception for small businesses.").

56 Byun, *supra* note 7, at 248.

57 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150(a)(1) (West 2022).

58 *Id.* § 1798.150(b) ("[I]f within [ ] 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.").

59 *Id.*

60 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.150 (West 2022).

consumers may sue the businesses responsible for permitting unauthorized access to or disclosure of their personal information.

Moreover, the CPRA grants enforcement authority to the newly established California Privacy Protection Agency (CPPA).[61] The agency is charged with administering, implementing, and enforcing the law; adopting regulations and providing guidance to both consumers and businesses; promoting public awareness and understanding of the law; monitoring the development of relevant technology; and performing "all other acts . . . appropriate . . . to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses."[62]

Accordingly, the CCPA and CPRA have laid the groundwork for a system of regulating the largely unimpeded collection and usage of consumer data that businesses once enjoyed. And through their comprehensive nature, these two laws have redefined U.S. data privacy for years to come.

B. The Virginia Consumer Data Protection Act ("VCDPA")

In early 2021, the Virginia legislature followed California by passing the Virginia Consumer Data Protection Act ("VCDPA"),[63] which was largely modeled after the failed Washington Senate Bill 5062.[64] The VCDPA incorporates many aspects of the California laws[65] but deviates in several notable respects.[66] Importantly, the VCDPA offers an example of how other states may

---

[61] *Id.* § 1798.155(b) ("Any business . . . that violates this title shall be subject to an injunction and liable for a civil penalty . . . which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.").

[62] *Id.* § 1798.199.40.

[63] Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2022).

[64] *See* VA. CONSUMER DATA PROT. ACT WORK GRP. OF THE JOINT COMM'N ON TECH. & SCI., 2021 FINAL REPORT3, https://rga.lis.virginia.gov/Published/2021/RD595/PDF (last visited Sept. 19, 2022) ("The VCDPA was modeled on SB 5062 in Washington, which failed to pass the Washington State Legislature" in early 2021.).

[65] K. Royal, P*rivacy Now: What in the [Privacy] World is Happening*?, ACC DOCKET, at *4 (Mar. 31, 2021) ("[The VCDPA] carries many similarities to the CCPA . . ., but several notable differences.").

[66] *Id*. Unlike the CCPA and CPRA, the VCDPA requires businesses to obtain affirmative consent from the consumer before processing sensitive consumer data; restricts the consumer's right to opt-out to the processing of their data for purposes of third-party sales, targeted advertising, and certain profiling activities; excludes a minimum annual gross revenue threshold for determining applicability; adds explicit requirements for data protection assessments and data minimization practices; and excludes a private right of action for consumers. *See* Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2022).

take a piecemeal approach to integrating elements of the CCPA and CPRA into their own data privacy legislation.[67]

1. Scope of Protection

Like the CCPA and CPRA, "personal data" is defined in a very broad fashion under the VCDPA: "[a]ny information that is linked or reasonably linkable to an identified or identifiable natural person."[68] The VCDPA also follows the California laws by excluding publicly available information[69] as well as certain medical,[70] financial,[71] educational,[72] and employment[73] data from its purview. And with respect to entities, state institutions,[74] nonprofit organizations,[75] institutions of higher education,[76] and certain financial institutions[77] are exempted from compliance.

Moreover, the VCDPA distinguishes between "personal data" and "sensitive data" in a manner similar to the CPRA.[78] Under the VCDPA, "sensitive data" is defined to include personal data revealing race, religion, health, sexual orientation, or citizenship; genetic or biometric data; precise geolocation data; and the personal data of a minor.[79] However, unlike the CPRA, the VCDPA includes an extra layer of protection for sensitive data by requiring

---

67 *See* Tobón, *supra* note 12 (noting that "[w]hile similar in scope to the CCPA, the VCDPA differs in its approach to regulating personal information").

68 Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 (West 2022).

69 *Id.* (defining "publicly available information" as "information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media . . . unless the consumer has restricted the information to a specific audience").

70 *Id.* §§ 59.1-572(C)(1)–(3), (9) (exempting "[p]rotected health information under HIPAA," "[h]ealth records for purposes of Title 32.1," patient identifying information, and "[i]nformation used only for public health activities and purposes as authorized by HIPAA").

71 *Id.* § 59.1-572(B)(ii) (exempting "financial . . . data subject to Title V of the federal Gramm-Leach-Bliley Act").

72 *Id.* § 59.1-572(C)(12) (exempting "[p]ersonal data regulated by the federal Family Educational Rights and Privacy Act").

73 *Id.* § 59.1-572(C)(14) (exempting "[d]ata processed or maintained . . . in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a [business]").

74 *Id.* § 59.1-572(B)(i) (exempting "any [ ] body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth").

75 *Id.* § 59.1-572(B)(iv).

76 *Id.* § 59.1-572(B)(v).

77 *Id.* § 59.1-572(B)(ii) (exempting "any . . . financial . . . institutions subject to Title V of the federal Gramm-Leach-Bliley Act").

78 *Id.* § 59.1-575.

79 *Id.*

that businesses obtain affirmative consent from the consumer before "processing"[80] such data.[81]

2. Consumer Rights

The VCDPA parallels the CCPA and CPRA by granting an assortment of individual rights to consumers over their personal data following collection.[82] Under the VCDPA, consumers are given (1) a right to access their personal data as processed by businesses;[83] (2) a right to direct businesses to delete their personal data;[84] (3) a right to opt-out of the processing of personal data for purposes of third-party sales, targeted advertising, or profiling;[85] (4) a right to direct businesses to correct inaccurate personal data;[86] and (5) a right against discrimination in the price or quality of products should they choose to exercise their rights under the law.[87]

However, the consumer right to opt-out under the VCDPA likely encompasses a narrower set of processing activities than the right to opt-out under the CPRA. While the CPRA broadly enables consumers to opt-out of the sale or "sharing"[88] of their consumer data,[89] the VCDPA limits the breadth of this right to processing for purposes of third-party sales, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[90] In doing so, the VCDPA offers consumers

---

80 *Id.* § 59.1-571 (defining "processing" as "any operation or set of operations performed, whether by manual or automated means, on personal data . . . such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data").

81 *Id.* § 59.1-574(A)(5) ("[A business] shall . . . [n]ot process sensitive data concerning a consumer without obtaining the consumer's consent."); Tobón, *supra* note 12 ("[The VCDPA] creates an opt-in regime for the processing of sensitive personal information.").

82 VA. CODE ANN. §§ 59.1-573, 59.1-574 (West 2022).

83 *Id.* §§ 59.1-573(A)(1), (4).

84 *Id.* § 59.1-573(A)(3).

85 *Id.* § 59.1-573(A)(5).

86 *Id.* § 59.1-573(A)(2).

87 *Id.* § 59.1-574(A)(4).

88 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.140(ah)(1) (West 2022) (defining "sharing" as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.").

89 *Id.* § 1798.120(a).

90 VA. CODE ANN. § 59.1-573(A)(5) (West 2022); *see also id.* § 59.1-571 (defining "[d]ecisions that produce legal or similarly significant effects concerning a consumer" as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water").

control over a well-defined set of processing activities while allowing businesses latitude in other uses of consumer data.

3. Applicability

Although the VCDPA implements the threshold framework created by the CCPA to determine the law's applicability to businesses, it modifies several of these thresholds.[91] Under the VCDPA, an entity that conducts business in the state or targets residents with its products is required to comply if it meets one or more of the following thresholds: (1) annually controls or processes the personal data of at least 100,000 consumers; or (2) annually controls or processes the personal data of at least 25,000 consumers and derives over 50% of its gross revenue from the sale of such data.[92]

Thus, the VCDPA eliminates the minimum annual gross revenue threshold found in the California laws. This modification may lead to fewer small businesses being required to comply with the law.[93] The Virginia state legislature also added a minimum processing threshold that must be met before a business that derives at least 50% of its annual gross revenue from selling personal data becomes subject to the law.[94] Collectively, these threshold adjustments may subject a smaller proportion of businesses to the VCDPA than the California laws.

4. Additional Business Obligations

The VCDPA also expressly places several additional obligations on businesses required to comply with the law. First, the VCDPA mandates data protection assessments[95] to be conducted for processing activities that present a heightened risk of consumer harm,[96] thereby adding another layer of protection against the misuse of consumer data collected by businesses. Second, the

91 *Id.* § 59.1-572(A).

92 *Id.*

93 *See* Byun, *supra* note 7, at 249.

94 VA. CODE ANN. § 59.1-572(A) (West 2022).

95 *Id.* § 59.1-576(B) (requiring that data protection assessments "identify and weigh the benefits that may flow . . . from the processing . . . against the potential risks to the rights of the consumer . . . as mitigated by safeguards that can be employed by the controller to reduce such risks").

96 *Id.* § 59.1-576(A) (requiring data protection assessments to be conducted for the processing of personal data for purposes of (1) third-party sales; (2) targeted advertising; (3) profiling that "presents a reasonably foreseeable risk of . . . substantial injury to consumers"; (4) the processing of sensitive data; and (5) other processing activities that "present a heightened risk of harm to consumers").

VCDPA places businesses under a duty to practice data minimization,[97] to implement and maintain appropriate data security practices,[98] and to disclose processing activities for purposes of third-party sales or targeted advertising.[99] These obligations will increase the cost of compliance, a concern already shared by businesses subject to the California laws.[100]

5. Enforcement

Finally, the VCDPA contradicts the CCPA and CPRA by excluding a private right of action for consumers.[101] Instead, the state Attorney General is given exclusive authority to enforce the VCDPA against businesses.[102] This enforcement framework was identified by the VCDPA Work Group of the Joint Commission on Technology and Science as a major reason for passage: "[an] important strategic distinction[ ] that led to the successful passage of the [VCDPA] . . . , as opposed to similar legislative efforts in other states . . . , remain[s] . . . the enforcement of the law by the Attorney General."[103] However, the VCDPA does follow the California laws by offering businesses a 30-day grace period to cure violations before an enforcement action may be brought by the Attorney General.[104]

In sum, the Virginia legislature utilized a majority of the template established by the California laws when drafting the VCDPA but deviated in areas where the legislature found alternative methods of consumer protection appropriate. This practice is likely to be replicated by other state legislatures as they undertake the process of drafting data privacy legislation tailored to their own state.

---

97 *Id.* § 59.1-574(A)(1) ("[A business] shall . . . [l]imit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer . . . .").

98 *Id.* § 59.1-574(A)(3) ("[A business] shall . . . [e]stablish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.").

99 *Id.* § 59.1-574(D).

100 Alexandria Henry, *The California Consumer Privacy Act's Potential Incompatibility with the United States' Legal and Economic Landscape*, 23 SMU SCI. & TECH. L. REV. 227, 248 (2020) (noting that "[t]he CCPA's extraterritorial effect on companies in the United States may create unintended consequences for smaller businesses and industries that may be unable to keep up with the cost of compliance and additional burdens imposed on them.").

101 VA. CODE ANN. § 59.1-580(E) (West 2022) (providing that "[n]othing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action to violations of this chapter or under any other law.").

102 *Id.* § 59.1-580(D).

103 2021 FINAL REPORT, *supra* note 64, at 7.

104 VA. CODE ANN. § 59.1-579(B) (West 2022).

C. The Colorado Privacy Act ("CPA")

Several months after the VCDPA was passed, the Colorado state legislature passed the Colorado Privacy Act ("CPA")[105] to become the third state with a comprehensive data privacy law.[106] Following the approach taken by the VCDPA, the CPA incorporates many components of the CCPA but differs in certain respects where necessary to best tailor its provisions to the residents of Colorado.[107]

1. Scope of Protection

Like the data privacy laws discussed above, the CPA's definition of "personal data" encompasses a wide variety of information concerning consumers.[108] The CPA also remains consistent with other laws by excluding certain types of consumer data from its purview as well as exempting certain entities from compliance.[109]

In defining personal data, the CPA distinguishes between ordinary personal data and "sensitive data."[110] Following the VCDPA's approach, the CPA requires businesses to obtain affirmative consent from consumers prior to processing[111] sensitive data.[112] The CPA also prohibits the processing of sensitive

---

105 Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301–6-1-1313 (West 2022).

106 John Fitzgerald, *Colorado Lawmakers Approve Landmark Data Privacy Bill*, WESTLAW DATA PRIV. DAILY BRIEFING (June 9, 2021).

107 F. Scott Galt, Romaine C. Marshall, & Casey E. Waughn, *United States: Data Privacy's Patchwork Expands*, MONDAQ BUSINESS BRIEFING (Sept. 29, 2021) ("While [the Colorado Privacy Act] is similar to Virginia and California's data privacy statutes, there are some distinct differences . . . ."). Unlike the CCPA and CPRA, the CPA requires businesses to obtain affirmative consent from the consumer and conduct a data protection assessment before processing sensitive consumer data; establishes a deadline for businesses to enable a global privacy control browser opt-out mechanism; excludes a minimum annual gross revenue threshold for determining applicability; adds explicit requirements for data protection assessments and data minimization practices; and excludes a private right of action for consumers. *See* Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301–6-1-1313 (West 2022).

108 Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303(17) (West 2022) (defining "personal data" as "information that is linked or reasonably linkable to an identified or identifiable individual.").

109 *See id*. § 6-1-1304(2).

110 *Id.* § 6-1-1303(24) (defining "sensitive data" as "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; [ ] genetic biometric data . . . ; or [ ] personal data from a known child").

111 *Id.* § 6-1-1303(18) (defining "processing" as "the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data").

112 *Id.* § 6-1-1308(7) ("A [business] shall not process a consumer's sensitive data without first obtaining the consumer's consent . . . .").

data without conducting a data protection assessment.[113] Accordingly, the scope of protection provided to consumers over their personal data under the CPA closely resembles that of the VCDPA.

2. Consumer Rights

The bundle of consumer rights granted by the CPA largely resemble those provided under the CCPA, CPRA, and VCDPA. Unlike any other law, however, the CPA provides a deadline by which businesses must enable consumers to opt-out through a "global privacy control browser, rather than on a website-by-website basis"[114] (July 2024).[115] This requirement is presumably aimed at preventing the "notification fatigue" that some worry may accompany the website-by-website opt-out scheme established by the CCPA.[116]

3. Applicability

With respect to applicability, an entity that conducts business within the state or intentionally targets residents with products is required to comply with the CPA if it meets one or more of the following thresholds: (1) annually controls or processes the personal data of at least 100,000 consumers; or (2) annually controls or processes the personal data of at least 25,000 consumers and "derives revenue or receives a discount . . . from the sale of personal data."[117] Accordingly, the CPA resembles the VCDPA by excluding the minimum annual gross revenue threshold present in the CCPA and CPRA. Moreover, in its second threshold, the CPA omits the minimum percentage of revenue requirement found in other laws and incorporates a minimum processing element akin to the one included in the VCDPA.[118]

---

[113] *Id.* § 6-1-1309(1) ("A [business] shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment . . . ."); *see also Id.* § 6-1-1309(2) (defining "processing that presents a heightened risk of harm" as including the processing of sensitive data).

[114] Galt, Marshall & Waughn, *supra* note 107 ("By 2024, companies must allow consumers to opt out through a global privacy control browser, rather than on a website-by-website basis.").

[115] Colorado Privacy Act, COLO. REV. STAT. § 6-1-1306(1)(a)(IV)(B) (West 2022) ("Effective July 1, 2024, a [business] that processes personal data for purposes of targeted advertising or the sale of personal data shall allow consumers to exercise the right to opt out . . . through a user-selected universal opt-out mechanism . . . .").

[116] 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/ ("One sticking point of the current opt-out system is notification fatigue. When every app and website is asking you for dozens of permissions, it becomes easier to accept the status quo than to manually opt out of every tracking technology.").

[117] Colorado Privacy Act, COLO. REV. STAT. § 6-1-1304(1) (West 2022).

[118] *Id.*

4. Additional Business Obligations

The CPA also places businesses under many of the same additional obligations as the VCDPA. Under the CPA, businesses are required to conduct data protection assessments[119] for any "[data] processing that presents a heightened risk of harm to a consumer."[120] Additionally, the CPA places businesses under a duty of data minimization, transparency, purpose specification, and data security.[121] Like the VCDPA, these miscellaneous business obligations provide extra layers of protection for consumer data while substantially increasing the cost of compliance.

5. Enforcement

Finally, the CPA follows the VCDPA by omitting a private right of action for consumers.[122] Instead, the CPA provides for joint enforcement by the state Attorney General and District Attorneys.[123] Moreover, the CPA offers businesses an increased grace period of 60 days to cure violations before becoming subject to liability.[124] However, this cure period is set to be repealed on January 1, 2025.[125]

Accordingly, Virginia and Colorado have incorporated supplemental elements of data protection into the general framework established by the CCPA and CPRA. With this precedent set, the West Virginia legislature would be wise to employ a similar technique in crafting its own comprehensive data privacy law.

---

[119] *Id.* § 6-1-1309(3) (requiring an assessment balancing the benefit of data processing activities against the risk of harm presented to consumers as a result of such processing).

[120] *Id.* § 6-1-1309(2) (defining "processing that presents a heightened risk of harm to a consumer" to include processing for purposes of (1) targeted advertising; (2) third-party sales; (3) profiling that presents a reasonably foreseeable risk of substantial injury to consumers; and (4) the processing of sensitive data.").

[121] *Id.* § 6-1-1308.

[122] *Id.* § 6-1-1310(1) ("[The CPA] does not authorize a private right of action for a violation of this [Act] or any other provision of law.").

[123] *Id.* § 6-1-1311(1)(a).

[124] *Id.* § 6-1-1311(1)(d).

[125] *Id.*

D. Pending Data Privacy Legislation

A number of states have introduced comprehensive data privacy bills that were still pending in the state legislature as of March 2022.[126] Like the VCDPA and CPA, these bills propose to incorporate the general structure set forth by the CCPA and CPRA but diverge in certain areas in order to tailor protection to their residents. This section will examine these bills and further delineate the legislative trends accompanying the nation's movement toward comprehensive data privacy laws.

1. Scope of Protection

Like the laws discussed to this point, data privacy bills introduced by the Minnesota, North Carolina, Ohio, Pennsylvania, and New York state legislatures would define personal data in a sweeping manner, including many of the same categories of personal information seen in the California laws.[127] Each bill would also exempt specified entities, such as governments and entities covered by HIPAA, and data, such as certain financial, medical, employment, and educational information.[128] Accordingly, these bills resemble the CCPA by generally "cast[ing] a wide net"[129] of protection but restricting the ultimate reach of the law through exemptions.

However, inconsistency arises in the extent of protection that these bills propose to offer for sensitive personal data. Unlike the CPRA, VCDPA, and CPA, several of these bills would not distinguish between ordinary and sensitive personal data: Ohio House Bill No. 376, Pennsylvania House Bill 1126, and New York Senate Bill 6701 each intend to treat all personal data the same.[130] To the contrary, Minnesota House Bill 1492 and North Carolina Senate Bill 569 aim to include heightened protection for "sensitive" personal data, which defines this

---

126 *See, e.g.*, H.B. 1492, 92d Leg., Reg. Sess. (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021).

127 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.02(m) (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1100(16) (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-70(a)(19) (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. § 1355.01(J) (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 3 (Pa. 2021).

128 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.03(2) (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1101(2) (N.Y. 2021); S.B. 569 2021 Gen. Assemb., Reg. Sess. §§ 75-70(c), (d) (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. § 1355.02(B) (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 3 (Pa. 2021).

129 Byun, *supra* note 7, at 248.

130 *See* S.B. 6701, 2021 Gen. Assemb., Reg. Sess. (N.Y. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021).

category of information in largely the same way as the laws discussed above.[131] And like the VCDPA and CPA, these bills would require businesses to obtain affirmative consent from consumers before processing their sensitive personal data.[132] They would also require businesses to conduct a data protection assessment for such processing.[133]

Accordingly, while these pending data privacy bills are consistent in defining what personal data is entitled to protection, they often vary in the degree of protection extended to "sensitive" personal data.

2. Consumer Rights

Like the laws surveyed above, each of these bills proposes to grant consumers an assortment of rights over their personal data. In general, these bills would grant consumers a right to access; a right to deletion; a right to opt-out of certain processing activities; and a right against discrimination if they choose to exercise their rights under the law.[134] Additionally, the bills in Minnesota, North Carolina, and New York seek to grant consumers a right to correct inaccuracies in their personal data following collection.[135]

Despite the apparent similarity in the consumer rights extended under these bills, the breadth of the consumer right to opt-out remains a source of inconsistency. The bills in Ohio and Pennsylvania resemble the CCPA by proposing to allow consumers to opt-out of the sale of their personal data.[136] On the other hand, the Minnesota and North Carolina bills would adopt the model established by the VCDPA and CPA and offer a right to opt-out of the processing of personal data for purposes of third-party sales, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects.[137] Finally, the New York bill would require businesses to obtain opt-in

---

131 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.02(S) (Minn. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-70(a)(28) (N.C. 2021).

132 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.07(2)(e) (Minn. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-72(a)(5) (N.C. 2021).

133 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.08(a)(3) (Minn. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-74(a)(4) (N.C. 2021).

134 *See* H.B. 1492, 92d Leg., Reg. Sess. §§ 325O.05, 325O.07(3) (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1102(5) (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. §§ 75-71(a), 75-72(a)(4) (N.C. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. §§ 1355.03–1355.07 (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 4(a) (Pa. 2021).

135 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.05(1)(c) (Minn. 2021); S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1102 (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-71(a)(2) (N.C. 2021).

136 *See* H.B. 376, 134th Gen. Assemb., Reg. Sess. § 1355.06 (Ohio 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 4(a)(3) (Pa. 2021).

137 *See* H.B. 1492, 92d Leg., Reg. Sess. § 325O.05(1)(f) (Minn. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-71(a)(5) (N.C. 2021).

consent from consumers before processing their personal data,[138] a requirement not seen in any of the data privacy laws discussed above.

Therefore, although each of these bills generally grants the consumer rights seen in the CCPA and CPRA, some also deviate from that template to offer additional rights and/or modify the accompanying obligations placed on businesses.

3. Applicability

To determine applicability, the bills incorporate the threshold framework created by the CCPA. However, the degree of similarity between the specific thresholds and those included within the CCPA varies from bill to bill. The Ohio bill seeks to require compliance from businesses that meet thresholds almost identical to those included within the CCPA (as amended by the CPRA).[139] The New York bill would employ the same thresholds while adding an unfamiliar fourth: compliance is required from any business that controls or processes personal data of at least 500,000 people nationwide, of which 10,000 are New York residents.[140] This fourth threshold in the New York bill is not found within any other data privacy law to date. Similarly, the Pennsylvania bill seeks to implement the thresholds found in the CCPA but would reduce the minimum annual revenue threshold to $10,000,000.[141]

On the other hand, the bills in North Carolina and Minnesota are more akin to the VCDPA in this respect. The North Carolina bill seeks to include thresholds nearly identical to those under the VCDPA.[142] The Minnesota bill differs slightly by seeking to reduce the percentage of revenue derived from the sale of personal data in the second threshold of the VCDPA from 50% to 25%.[143]

Thus, the applicability thresholds proposed by these data privacy bills do not stray too far from those included within the data privacy laws discussed in the previous section. Several of the bills have chosen to implement thresholds

---

138 *See* S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1102(2) (N.Y. 2021).

139 H.B. 376, 134th Gen. Assemb., Reg. Sess. § 1355.02 (Ohio 2021) (very similar to the CPRA, the Ohio bill would apply to businesses that meet one or more of the following thresholds: (1) earns at least $25,000,000 in annual gross revenue; (2) annually controls or processes personal data of at least 100,000 consumers; or (3) annually controls or processes personal data of at least 25,000 consumers and derives more than 50% of its gross revenue from the sale of such data.).

140 S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1101(1) (N.Y. 2021).

141 H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 3(1)(iv)(A) (Pa. 2021).

142 S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-70(b) (N.C. 2021) (the North Carolina bill would apply to businesses that meet one or more of the following thresholds: (1) annually controls or processes personal data of at least 100,000 consumers; or (2) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data).

143 H.B. 1492, 92d Leg., Reg. Sess. § 325O.03 (Minn. 2021).

resembling those found within the CCPA and CPRA, while others have chosen to rely on the model established by the VCDPA and CPA.

4. Enforcement

In terms of enforcement, data privacy bills can be divided into two categories: those that authorize a private right of action and those that do not. The bills in Pennsylvania, North Carolina, and New York would provide for a private right of action against businesses responsible for breaches of consumer data, subject to certain limitations.[144] Under the Pennsylvania bill, this limited private right of action is identical to the one within the CCPA, including its inclusion of a 30-day grace period for businesses to cure violations.[145] The New York bill deviates slightly from the CCPA by proposing to limit the private right of action to consumers who have been denied the ability to exercise their consumer rights under the law.[146]

Meanwhile, the bills in Minnesota and Ohio would follow the VCDPA and CPA by omitting a private right of action and providing for exclusive enforcement by the state Attorney General.[147] Each also includes a 30-day grace period for businesses to cure violations before an enforcement action could be instituted by the Attorney General.

In sum, a number of states have opted for the approach first employed by the Virginia and Colorado legislatures when drafting the VCDPA and CPA: adopting the basic framework created by the CCPA but altering it in areas where a different form of protection would best suit its residents. The frequency with which this technique is employed adds strength to the conclusion that the West Virginia legislature is likely to use a similar method to create its own data privacy law.

E. Failed Data Privacy Legislation

Notwithstanding the legislation analyzed to this point, many states have failed in their attempt to enact a comprehensive data privacy law.[148] These bills appear to have failed for various reasons, with each including unconventional

144 *See* S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1106(6) (N.Y. 2021); S.B. 569, 2021 Gen. Assemb., Reg. Sess. § 75-77(b) (N.C. 2021); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 4(n) (Pa. 2021).

145 *See* H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 4(n) (Pa. 2021).

146 *See* S.B. 6701, 2021 Gen. Assemb., Reg. Sess. § 1106(6) (N.Y. 2021).

147 H.B. 1492, 92d Leg., Reg. Sess. § 325O.10 (Minn. 2021); H.B. 376, 134th Gen. Assemb., Reg. Sess. § 1355.09(A) (Ohio 2021).

148 *See, e.g.*, H.B. 216, 2021 Gen. Assemb., Reg. Sess. (Ala. 2021); H.B. 969, 2021 Gen. Assemb., Reg. Sess. (Fla. 2021); H.R. 3741, 87th Leg., Reg. Sess. (Tex. 2021); S.B. 5062, 2021 Gen. Assemb., Reg. Sess. (Wash. 2021).

features as compared to the CCPA, CPRA, VCDPA, and CPA. This section will explore the differences between these unsuccessful bills and the data privacy laws discussed above, identifying characteristics that may have prevented the unsuccessful bills from becoming law.

1. Scope of Protection

Texas House Bill 3741 illustrates that too much deviation from the definition of personal information established by the CCPA and CPRA may present a hurdle to passage. Rather than broadly defining personal data and then offering stronger protection for sensitive personal data, this bill sought to define three categories of personal data with varying levels of protection.[149]

"Category one information," which was offered no additional protection, was defined as personal data that an individual "may use in a personal, civic, or business setting," including government-issued identification numbers, financial account numbers, biometric information, and health information.[150] "Category two information," which businesses could not sell or share to third parties, was defined as personal data that presented a privacy risk to consumers.[151] This category included information concerning age, race, religion, and geolocation.[152] Finally, "category three information," which businesses could not collect at all, was defined to include personal data concerning time of birth and political association.[153]

By proposing to protect consumer data in this manner, the bill may have created restrictions that were too harsh on businesses in comparison to other data privacy laws. This may be especially true in the bill's prohibition against the sale or sharing of "category two information."

2. Applicability

Alabama House Bill 216 presents an example of how an extremely broad application to businesses may similarly hinder chances of passage. Rather than implementing the threshold framework found in other laws to determine applicability, this bill would have applied to any for-profit entity that conducts business in the state, collects consumer data, and determines the purposes and means for processing that data.[154]

---

149 H.R. 3741, 87th Leg., Reg. Sess. §§ 541.001(2)–(4) (Tex. 2021).

150 *Id.* § 541.001(2).

151 *Id*. § 541.001(3).

152 *Id.*

153 *Id*. § 541.001(4).

154 H.B. 216, 2021 Gen. Assemb., Reg. Sess. § 2(3)(a) (Ala. 2021).

By doing so, the bill presumably would have applied to many small businesses qualifying for exemptions in other laws.[155] Similarly, the bill would have applied to businesses that only collect a trivial amount of consumer data without generating a substantial profit. As a result, this bill almost certainly encountered a great deal of criticism from businesses that would fall within exemptions carved out by other data privacy laws.

3. Enforcement

Finally, the fates of Washington Senate Bill 5062 and Florida House Bill 969 demonstrate that a bill may not survive the legislative vetting process due to disagreement over the inclusion of a private right of action. Each failed to garner enough support for passage in large part due to irreconcilable differences in the legislature over whether individual consumers should be able to bring lawsuits against businesses that violate their privacy rights.[156]

Therefore, a data privacy bill venturing too far from the model created by the CCPA and CPRA may encounter increased resistance and hesitation from the state legislature. Accordingly, the West Virginia legislature is likely to place a heavy emphasis on integrating elements of the California laws into its own data privacy law.

III. W. VA. HOUSE BILL 3159 – FLAWS THAT MAY HAVE FORESTALLED PASSAGE

West Virginia House Bill 3159 represents the most recent attempt by the West Virginia state legislature at enacting a comprehensive data privacy law.[157] Although ultimately unsuccessful, the bill serves as a useful starting point for predicting the characteristics of a data privacy law in West Virginia. This section identifies several flaws that may have subjected House Bill 3159 to heavy criticism, providing an important basis for making these predictions.

---

155 *See* Byun, *supra* note 7, at 249.

156 H.B. 969, 2021 Gen. Assemb., Reg. Sess. (Fla. 2021); S.B. 5062, 2021 Gen. Assemb., Reg. Sess. § 111 (Wash. 2021); Scott Giordano & Jennifer K. Mailander, *Is U.S. Privacy Law Standing Still?*, ACC DOCKET (Sept. 20, 2021), https://docket.acc.com/us-privacy-law-standing-still ("a private right of action for aggrieved consumers is often cited as a sticking point (the proposed Washington Privacy Act . . .)"); Melody Lynch & Drew Sorrell, *Florida's Consumer Privacy Law Fails to Pass*, JD SUPRA (May 4, 2021), https://www.jdsupra.com/legalnews/florida-s-consumer-privacy-law-fails-to-1446735/ (the Florida Privacy Protection Act "largely failed to pass due to a disagreement between Florida's [H]ouse that wanted a private right of action included and the Florida Senate that wanted only Florida's Attorney General to have enforcement rights.").

157 H.B. 3159, 85th Leg., Reg. Sess. (W. Va. 2021).

A. Scope of Protection

Like the data privacy laws discussed earlier, House Bill 3159 sought to define "personal information" in an expansive manner: "information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being . . . associated or linked with a particular consumer or household."[158] However, unlike the CCPA and CPRA, all employment-related information[159] and non-public educational information[160] would have fallen within the purview of House Bill 3159. The only explicit exemptions would have concerned publicly available and de-identified information.[161] The absence of exemptions placed House Bill 3159 at odds with the CCPA, CPRA, VCDPA, and CPA, and it likely would have encountered serious criticism from businesses if enacted.

Moreover, House Bill 3159 would not have distinguished between ordinary and sensitive personal information, unlike the CPRA, VCDPA, and CPA.[162] Consumers would have received no additional protection for personal information revealing race, religion, health, sexual orientation, or citizenship; biometric data; or precise geolocation data. As a result, House Bill 3159 missed an opportunity to alleviate consumer concerns over the retention of sensitive consumer data by businesses,[163] which may have hindered the bill's chances at passage.

B. Consumer Rights

House Bill 3159 proposed to grant consumers a bundle of rights over their personal data that closely resembles those included within the data privacy laws examined above. First, the bill would have provided consumers with a right to access their personal information as collected by businesses.[164] Similarly, the law also sought to give consumers a right to know the categories of personal information sold or shared as well as the categories of third-party recipients.[165] Second, the bill would have included a consumer right to direct businesses to

---

158 *Id.* § 46A-9-1(a)(13) (defining "personal information" to include personal identifiers, characteristics of protected classifications, commercial information, biometric information, and internet activity information).

159 *Id.* § 46A-9-1(B)(1).

160 *Id.* § 46A-9-1(J).

161 *Id.*

162 *See generally id.*

163 *See* Martin, *supra* note 4, at 11 (noting that the findings of a recent focus group study of West Virginia residents showed that participants desired a data privacy law that "place[s] restrictions on who can collect sensitive data and how long they may retain the information").

164 H.B. 3159, 85th Leg., Reg. Sess. (W. Va. 2021).

165 *Id.* § 46A-9-5.

delete personal information following collection,[166] subject to a number of exceptions copied from the CCPA.[167] Third, like the CPRA, the bill would have granted consumers a right to direct businesses to use "commercially reasonable efforts" to correct inaccurate personal information maintained by the business.[168] Fourth, the bill would have extended a consumer right against discrimination in the price or quality of products if they choose to exercise their rights under the law.[169]

Fifth, like the CPRA, House Bill 3159 would have included a consumer right to opt-out of the sale or sharing of personal information with third parties.[170] The bill sought to place bounds on this right to opt-out by listing disclosures that would not be considered selling or sharing consumer data.[171] These exceptions would have included each of the following: disclosure at the direction of the consumer; disclosure to alert third parties of the consumer's desire to opt-out; and disclosure necessary to accomplish a merger, acquisition, or similar transaction.[172] Even after including these narrow exceptions, however, the bill's right to opt-out was likely to disturb a wider range of processing activities than the right to opt-out under the VCDPA and CPA.

C. Applicability

To determine which businesses were required to comply, House Bill 3159 would have employed a threshold system almost identical to that of the CCPA.[173] "Business" would have been defined as any for-profit entity that conducts business within the state, collects consumer data, and determines the purposes and means of processing that data.[174] The bill sought to require compliance from any business that met one or more of the following thresholds: (1) generates at least $25,000,000 in annual gross revenue; (2) annually buys, receives, sells, or shares for commercial purposes the personal information of at least 50,000 consumers; or (3) derives at least 50% of its annual gross revenue from selling or sharing the personal information of consumers.[175]

Once the VCDPA and CPA excluded a minimum annual gross revenue threshold, the inclusion of one here could have sparked resistance on behalf of

166 *Id.* § 46A-9-4(a).

167 *Id.* § 46A-9-4(c).

168 *Id.* § 46A-9-4(d).

169 *Id.* § 46A-9-7.

170 *Id.* § 46A-9-6(a).

171 *Id.* §§ 46A-9-6(e), (f).

172 *Id.*

173 *Id.* § 46A-9-1(a)(3).

174 *Id.*

175 *Id.*

small and medium-sized businesses.[176] Similarly, once the CPRA increased the second processing threshold of the CCPA to 100,000 consumers, placing its analogous threshold at 50,0000 consumers would have made House Bill 3159 inconsistent with other laws and would have likely encountered criticism from businesses that process the personal information of between 50,000 to 100,000 consumers.

D. Additional Business Obligations

Another feature of House Bill 3159 likely to face opposition was the absence of any explicit duty of businesses to practice data minimization by limiting their use of personal information to what is required to fulfill the purposes for which it was collected. Such a duty was included within both the VCDPA and CPA. The lack of one here may have created a potential loophole for businesses to process consumer data for undisclosed purposes under the pretext of its original avowed purpose. This loophole likely would have generated dissent on behalf of consumers, as incomplete disclosure remains a primary concern over the collection and use of consumer data by businesses.[177]

Additionally, House Bill 3159 would have excluded a requirement for businesses to conduct data protection assessments for processing activities that present a heightened risk of consumer harm. This omission would have placed House Bill 3159 at odds with the VCDPA and CPA, which require businesses to conduct these cost-benefit assessments for processing activities conducted for purposes of third-party sales, targeted advertising, and profiling.[178] The lack of such a requirement here may have been subject to criticism on behalf of consumers because these assessments assure contemplation of the risks associated with certain processing activities.

---

[176] *See* Byun, *supra* note 7; Alfred J. Saikali, *Cybersecurity Incidents and Data Privacy: Five Ways to Improve Florida's Proposed Privacy Law*, JD SUPRA (Feb. 24, 2021) https://www.jdsupra.com/legalnews/five-ways-to-improve-florida-s-proposed-5143051/ (arguing that "[i]t isn't difficult for an organization to hit the $25 million threshold. According to the U.S. Small Business Administration, many small businesses hit this requirement depending on their industry.").

[177] *See* Martin, *supra* note 4, at 13 (arguing in favor of a general principle of data minimization to be included within a data privacy law in West Virginia); Susan Goebel-Nolan, Alexander "Sandy" R. Bilus, Andrea Gehman & Jennee DeVore, *How to Build a Privacy Program from Scratch*, ACC DOCKET, (May 7, 2021), https://docket.acc.com/how-build-privacy-program-scratch (arguing that "[a] well-constructed privacy notice provides data subjects and regulators alike with an accurate, transparent reflection of your company's use of data in compliance with applicable law. A poorly constructed privacy notice invites the potential for complaints, regulatory scrutiny, and potential legal action.").

[178] *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1309(3) (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-580(A) (West 2022).

E. Enforcement

Finally, like the CPRA, House Bill 3159 would have authorized a private right of action for consumers whose "personal information or e-mail address, in combination with a password or security question and answer that would allow access to the account," is subject to unauthorized access or disclosure.[179] Consumers would have been able to seek monetary damages[180] as well as injunctive[181] or declaratory[182] relief. However, unlike the CPRA and other laws, House Bill 3159 would have omitted any grace period for businesses to cure violations before a consumer could institute a civil action. The absence of a grace period to cure violations would have almost certainly encountered heavy resistance from businesses and likely presented a barrier to passage.

The bill would have also granted enforcement authority to the West Virginia Division of Consumer Protection.[183] Unlike the private right of action, however, this enforcement authority would have been subject to a 30-day cure period.[184]

In sum, House Bill 3159 was vulnerable to criticism from several different angles. The aggregate effect of the flaws identified above arguably doomed the bill's prospects of becoming law. Accordingly, the West Virginia legislature is likely to prioritize remedying these concerns when drafting a data privacy bill in the future.

IV. RECOMMENDATIONS FOR A DATA PRIVACY LAW IN WEST VIRGINIA

Because House Bill 3159 failed to become law, West Virginia remains without a comprehensive data privacy law to protect consumer data from business exploitation. However, the recent activity by other states and mounting support for data privacy laws across the nation[185] lends support to the conclusion that West Virginia will eventually pass such a law. This section argues for the inclusion of several features that would remedy some of the weaknesses that may

---

179 H.B. 3159, 85th Leg., Reg. Sess. § 46A-9-10 (W. Va. 2021).

180 *Id.* § 46A-9-1(a)(1) (authorizing consumers to seek "[d]amages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater").

181 *Id.* § 46A-9-1(a)(2) (authorizing consumers to seek "[i]njunctive . . . relief, as the court deems proper.").

182 *Id.* (authorizing consumers to seek "declaratory relief, as the court deems proper").

183 *Id*. § 46A-9-11(a).

184 *Id.* § 46A-9-11(c).

185 *See* Migliorini, *supra* note 16, at 244 (arguing that the U.S. should prioritize a national data privacy law because "the emerging patchwork state legislation arising in the U.S. will only breed inconsistencies and future confusion and haze, thereby creating a labyrinth that is a nightmare to navigate").

have led to the downfall of House Bill 3159. These features include (1) a distinction between ordinary and sensitive personal data; (2) a right to opt-out of a well-defined range of processing activities; (3) an applicability framework requiring compliance only from businesses that collect and/or use a substantial amount of consumer data; (4) an explicit duty for businesses to practice data minimization and to conduct data protection assessments; and (5) a limited private right of action with a grace period for businesses to cure violations.

A. Scope of Protection – A Distinction Between Ordinary and Sensitive Data

First, a data privacy law in West Virginia should distinguish between ordinary and sensitive personal information. As evidenced by the presence of such a distinction in the CPRA, VCDPA, and CPA, this feature has become an essential element of comprehensive data privacy laws. The importance of this distinction exists in the "reputational, financial, or material harm to the consumer" that could result from unauthorized access to or disclosure of their sensitive data.[186] Thus, meaningful protection of sensitive personal information should be prioritized during the drafting process.

The question becomes the degree of protection appropriate for sensitive personal information. While consumers are given a right to direct businesses to limit the processing of their sensitive personal information under the CPRA,[187] the VCDPA and CPA offer even further protection by prohibiting any processing of this information without affirmative consent from the consumer.[188] Whatever approach is employed, a balance must be struck between the consumer interest in enhanced control over their most delicate data and the business interest in minimizing the restrictions placed on their usage of consumer data.

Here, the approach taken by the CPRA would be appropriate to achieve this balance. Granting consumers a right to limit the processing of their sensitive data to what is necessary to furnish products "reasonably expected by an average consumer"[189] would offer consumers substantial control over how businesses use their most delicate personal information. This approach would also work to alleviate consumer concerns over the retention and usage of their sensitive personal data by businesses.[190] At the same time, businesses would still have latitude in their usage of most consumer data. Accordingly, this approach offers

---

186 Tobón, *supra* note 12.

187 *See* California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.121 (West 2022).

188 *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1308(7) (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-578(A)(5) (West 2022).

189 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.121 (West 2022).

190 *See* Martin, *supra* note 4, at 11 (noting that the findings of a recent focus group study of West Virginia residents showed that participants desired a data privacy law that "place[s] restrictions on who can collect sensitive data and how long they may retain the information").

meaningful consumer protection without placing unnecessary burdens on business innovation using consumer data.

B. Consumer Rights – A Right to Opt-out of Certain Processing Activities

Second, the legislature should follow the VCDPA[191] and CPA[192] by limiting the consumer right to opt-out of the processing of personal data for purposes of third-party sales, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[193] A right to opt-out of certain processing activities has become an anchor for the bundle of consumer rights provided under data privacy laws in other states. Furthermore, West Virginia consumers have expressed their desire for such a feature.[194] However, an overly broad right to opt-out may unnecessarily inhibit the ability of businesses to innovate using consumer data. Thus, the legislature will again be forced to consider competing interests between consumers and businesses.

Although the original right to opt-out under the CCPA was limited to third-party sales, the CPRA significantly broadened this right by allowing consumers to opt-out of the sharing of personal information to third parties.[195] And because "sharing" is defined under the CPRA to cover a wide range of disclosures for advertising purposes, regardless of whether compensation accompanies disclosure,[196] a right to opt-out of this breadth may unduly restrict businesses' usage of consumer data in contexts that do not present unreasonable risks to the consumer.

Accordingly, the legislature should follow the VCDPA and CPA by providing well-defined boundaries to the right to opt-out, rather than arbitrarily limiting it to the "sharing" of consumer data. Furthermore, by including targeted advertising within the range of processing activities subject to a consumer opt-

---

191 Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-577(A)(5) (West 2022).

192 Colorado Privacy Act, COLO. REV. STAT. § 6-1-1306(1)(a)(I) (West 2022).

193 Under the VCDPA and CPA, "decisions that produce legal or similarly significant effects concerning the consumer" means "a decision made by the [business] that results in the provision or denial by the [business] of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water." Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303(10) (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-571 (West 2022).

194 *See* Martin, *supra* note 4, at 11 (noting that the findings of a recent focus group study of West Virginia residents showed that participants "wanted the option to opt-in or out of the collection and use of their personal data").

195 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.120 (West 2022).

196 *Id.* § 1798.140(ah)(1) (defining "sharing" as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration").

out, the law should relieve concerns over "prejudicial ad targeting" among West Virginia consumers.[197] This approach would again offer consumers increased control over the usage of their personal data but limit this control to what is necessary to shield consumer data from exploitation by businesses.

C. Applicability – Demanding Compliance Only from Businesses that Process a Substantial Amount of Consumer Data

Third, like the VCDPA[198] and CPA,[199] the law should employ a dual-threshold approach to applicability. Specifically, the law should only require compliance from businesses that conduct business in the state and meet one of the following thresholds: (1) annually control or process personal data from at least 100,000 consumers; or (2) annually control or process personal data from a reduced number of consumers but derive more than a certain percentage their annual gross revenue from the sale of this data. "Consumer" should be defined as residents of West Virginia acting in an individual or household context.

Setting the first threshold at 100,000 consumers would be consistent with analogous thresholds under the CPRA,[200] VCDPA,[201] and CPA.[202] This consistency may lessen the burden of navigating "the emerging patchwork [of] state legislation"[203] by making it easier to determine which laws interstate businesses must comply with. In doing so, this feature carries the potential to lower compliance costs for such businesses. With respect to the second threshold, the specific number of consumers and percentage of revenue figures should be determined by the legislature after consulting relevant statistics of businesses conducting business in the state. This would ensure that the law demands compliance from businesses that collect and/or use enough consumer data to generate a substantial risk of consumer harm while exempting those that do not.

By excluding the minimum annual gross revenue threshold present in the CCPA and CPRA, the law would avoid requiring compliance from many

---

197 *See* Martin, *supra* note 4, at 11 (noting that the findings of a recent focus group study of West Virginia residents showed that participants recommended a prohibition against "racial or socioeconomic-based targeting").

198 Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-576(A) (West 2022) (applying to businesses that (1) annually control or process personal data from at least 100,000 consumers; or (2) annually control or process personal data from at least 25,000 consumers and derive more than 50% of their gross revenue from the sale of personal data).

199 Colorado Privacy Act, COLO. REV. STAT. § 6-1-1304(1) (West 2022) (applying to businesses that (1) annually control or process personal data from at least 100,000 consumers; or (2) annually control or process personal data from at least 25,000 consumers and derive any percentage of revenue from the sale of personal data).

200 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.140(c) (West 2022).

201 Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-572(A) (West 2022).

202 Colorado Privacy Act, COLO. REV. STAT. § 6-1-1304(1) (West 2022).

203 Migliorini, *supra* note 16.

small businesses that do not rely on significant amounts of consumer data to operate.[204] The presence of such a threshold carries the potential to "affect small and medium-sized businesses that are not in the tech industry and may [only] collect a small amount of personal information."[205] This effect is often a direct result of the numerical limits chosen by state legislatures: "[i]t isn't difficult for an organization to hit the $25 million threshold. According to the U.S. Small Business Administration, many small businesses hit this requirement depending on their industry."[206]

Furthermore, requiring compliance from businesses that merely generate more than a certain amount of revenue does little to further the purpose behind a data privacy law. For example, the avowed purpose of the CPA is to "[e]mpower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate."[207] However, businesses that would not meet the processing thresholds set forth above likely do not collect enough consumer data to create the privacy risks these laws are aimed at mitigating. Thus, the inclusion of a CCPA-like minimum annual gross revenue threshold is not likely to bring business operations presenting significant privacy risks within the purview of the law. Accordingly, the omission of such a threshold defends against the risk of unnecessarily inhibiting business innovation.

D. Additional Business Obligations – A Duty to Practice Data Minimization and Conduct Data Protection Assessments

Fourth, the law should follow the model set by the VCDPA and CPA to place businesses under a couple of additional obligations. First, the law should include an explicit duty to practice data minimization by limiting processing to what is necessary to achieve the purpose for which it was collected. Second, the law should mandate data protection assessments for any processing activity that presents a heightened risk of consumer harm. As seen in the VCDPA[208] and CPA,[209] these processing activities should include the use of sensitive personal information and any processing for purposes of third-party sales, targeted advertising, or profiling in furtherance of decisions producing legal or similarly significant effects concerning the consumer. To encourage compliance, the law

---

204 *See* Byun, *supra* note 7, at 249 (arguing that the CCPA and CPRA's "low threshold [encompasses] more than just the data giants that inspired this stringent law. Consequently, businesses with limited resources ('small businesses') are further disadvantaged in the marketplace due to costs associated with compliance.").

205 Saikali, *supra* note 176.

206 *Id.*

207 Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301(1)(c)(I) (West 2022).

208 Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-576(a) (West 2022).

209 Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1309(1)–(2) (West 2022).

should require that businesses make these assessments available to the Attorney General and Division of Consumer Protection upon request.

The inclusion of these requirements would enhance the data security protocols that businesses must practice in order to comply with the law. By requiring data minimization, businesses would be prohibited from processing consumer data for undisclosed purposes, which inherently involve heightened security risks.[210] Furthermore, mandating transparency during processing may remove potential loopholes by which businesses could avoid compliance. Similarly, mandating data protection assessments requires businesses to perform a cost-benefit analysis for the processing activities that carry the highest risks of consumer harm.[211] Businesses would be forced to consider the likelihood of injury to consumers in deciding whether a processing activity is appropriate under the law.

A foreseeable criticism concerns the corresponding increases in the cost of compliance.[212] However, these requirements strike a balance between the consumer interest in ensuring their data is secure and the business interest in minimizing regulation of their collection and usage of consumer data. Moreover, these additional consumer protections may be a necessary counterpart to permitting businesses to process consumer data for purposes of targeted advertising and profiling, especially with respect to sensitive personal information.

E. Enforcement – A Private Right of Action Limited by a Cure Period

Finally, the law should authorize a dual system of enforcement. First, the law should follow the CCPA[213] and CPRA[214] by authorizing a private right of action for consumers whose non-encrypted personal information becomes subject to unauthorized access or disclosure. This would allow the victims of a data breach to sue the business responsible.

However, as seen with the failed data privacy bills in Washington and Florida, including a private right of action may spark disagreement in the legislature.[215] The absence of a private right of action was also noted as a key

---

210 *See* Goebel-Nolan, Bilus, Gehman, & DeVore, *supra* note 177.

211 *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1309(3) (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-576(B) (West 2022).

212 *See* Henry, *supra* note 100, at 249–50 (arguing that smaller businesses are not equipped to handle the high costs of compliance associated with the CCPA and "may also receive less attention from potential investors, which would restrict a company's ability to earn larger profits and build its capital for future growth.").

213 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150(a) (West 2022).

214 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.150(a) (West 2022).

215 *See* Lynch & Sorrell, *supra* note 156.

reason why the VCDPA was able to gain enough support to pass.[216] In order to reach a compromise with those in opposition of such a feature, the law should include a qualification that was noticeably absent from House Bill 3159: a grace period for businesses to cure violations before becoming subject to liability. This cure period should be no less than the 30 days authorized under the CCPA and CPRA.[217] The practical effect of the CCPA's cure period has substantially benefited businesses: as of July 2021, "75% of businesses acted to come into compliance within the 30-day statutory cure period."[218]

Second, the legislature should also vest authority in the state Attorney General and Division of Consumer Protection to enforce the law. The CCPA, CPRA, VCDPA, and CPA all contain such a provision.[219] The language of this provision should be broad enough to authorize an enforcement action against any business found in violation. However, like the private right of action, businesses should be offered a grace period to cure violations before becoming subject to liability in an enforcement action.

By employing this dual system of enforcement, the law would empower consumers to enforce its requirements against businesses in a limited range of circumstances while authorizing the government to do so in others. Furthermore, the inclusion of a private right of action would promote active participation by consumers in the protection of their consumer data, a common theme throughout the U.S. data privacy landscape.

V. CONCLUSION

As consumers lobby for increased protection against the misuse of their consumer data by businesses, states will continue to pursue comprehensive data privacy legislation. Currently, without such a law, the state of West Virginia is no exception. Accordingly, serious consideration must be given to the features that should characterize such a law.

House Bill 3159 presumably failed to pass due to its inability to offer purposeful consumer protection without unnecessarily inhibiting business innovation through the use of consumer data. As illustrated above, however, there is room for improvement throughout the bill. These shortcomings must be remedied in order to create a data privacy law that truly strikes a balance between the competing interests of consumers and businesses.

---

216 2021 FINAL REPORT, *supra* note 64, at 7.

217 California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.150(b) (West 2022).

218 *Regulatory Update*, 25 NO. 1 J. INTERNET L. 3 (Aug. 2021).

219 *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.155(b) (West 2022); California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.155(b) (West 2022); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1311 (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-580 (West 2022).

To resolve these issues, the West Virginia state legislature should consult the data privacy laws successfully passed in other states. The CCPA, as amended by the CPRA, remains the fountainhead from which future data privacy legislation should flow. Furthermore, the VCDPA and CPA provide a model for future state legislatures to follow when selecting which elements of the California laws to integrate into their own law and which elements to deviate from. The features embodied in pending legislation from other states add to the propriety of this approach. Accordingly, the West Virginia legislature should begin with the template established by the CCPA and CPRA but depart from it where policy considerations within the state are appropriate.

Utilizing this approach, the West Virginia state legislature should aspire to create a comprehensive data privacy law characterized by several important features. First, the law should distinguish between ordinary and sensitive consumer data while extending an extra layer of protection to the latter. Second, the consumer right to opt-out under the law should be limited to a well-defined range of processing activities, such as for purposes of third-party sales, targeted advertising, or profiling. Third, the law should only require compliance from businesses that process a certain amount of consumer data or earn a substantial percentage of their revenue from the sale of consumer data. Fourth, businesses should be required to practice data minimization and conduct data protection assessments for processing activities that present a heightened risk of consumer harm. Finally, the law should authorize a limited private right of action for consumers whose personal information becomes subject to unauthorized access or disclosure, qualified by a grace period for businesses to cure violations.

By doing so, the West Virginia state legislature would exact a compromise between consumers and businesses. Adding an extra layer of protection for sensitive consumer data, requiring data minimization and data protection assessments, and including a private right of action would favor consumers. However, placing well-defined boundaries on the consumer right to opt-out, limiting application to businesses that process a significant amount of consumer data, and offering a cure period would favor businesses. In achieving this balance, the law would offer meaningful protection sufficient to remedy the power imbalance between consumers and businesses without unreasonably hindering business innovation.

Harrison Enright[*]

[*] Harrison Enright is a third-year law student at the West Virginia University College of Law. He would like to thank the members of the West Virginia Law Review for their hard work and valuable insight in preparing this student note for publication.