Volume 127 | Issue 2 Article 1

1-14-2025

The Law of Unintended Consequences: Examining West Virginia's Data Privacy Legislation and What Could Have Been

Jena Martin
St. Mary's University School of Law

Erin Kelley
West Virginia University

THE LAW OF UNINTENDED CONSEQUENCES: EXAMINING WEST VIRGINIA'S DATA PRIVACY LEGISLATION AND WHAT COULD HAVE BEEN[1]

Jena Martin & Erin Kelley+*

INTRODUCTION

The year is 2025. In this alternate universe, Unrepresented has become the hottest new social media network.[2] *Originating in the D.C. area, it quickly became popular with teens and young adults. After an explosion of growth, the*

---

[1] Much of the work in this essay grew out of concerns Prof. Martin encountered while researching West Virginia's data privacy bill in connection with an update to her 2021 paper on data privacy. *See* Jena Martin, Data Privacy Issues in West Virginia and Beyond: An Overview, 2d ed. (June 30, 2024) (unpublished white paper) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896449).

* Professor of Law and Katherine A. Ryan Chair of International and Global Law, St. Mary's University. This Essay is supported, in part, by St. Mary's Faculty Support Grant. Previously, Professor Martin served as the Robert A. Shuman Professor of Law and Ethics at West Virginia University, where she was a member of the faculty from 2009–2024. The authors would like to thank the following people for their insight and support: Justin Seybert, Kendra Fershee, Adam MacLeod, Jonathan Marshall, and Elaine Waterhouse Wilson.

+ Adjunct Faculty, West Virginia University. Previously Ms. Kelley was the Executive Director of the Teaching and Learning Commons at West Virginia University, where she consulted on matters of student privacy, intellectual property, and digital accessibility.

[2] Straight out of Ms. Kelley's Social Media and the Law course.

company decided to move its principal place of business to "State C."[3] *While the site was originally intended to be a place to discuss political action for those who couldn't vote, it has since grown to cover many different topics through an active network of both public and private groups.*

Sarah S. has been working through a sensitive, confidential, and relatively obscure medical condition. To find answers, she has spent her time surfing the internet, including exploring the public portions of the Unrepresented site.

When Sarah sees that there are some private groups for users who share her condition, she decides to become a member of the site. As part of the account creation process, Sarah accepts the Unrepresented user agreement, which comes up in a scrollable text box for her to read. Not thinking much of it, she quickly scrolls through the terms (without reading them) and clicks the checkbox that she "agrees" with the terms and conditions so that the button to "Create" her account becomes active. She then proceeds to use her account, joining a few of those private groups, where she discusses her condition in detail in order to solicit advice on the best medical doctors in the area.

Later, Sarah discovers that Unrepresented used her posts (in contravention of their terms and conditions)[4] *in public advertisements to show how Unrepresented connects people across the country. Although most of the information from her post was redacted, some identifying information was used, and soon people were mentioning her, by name, in public posts. Because of this, Sarah has suffered untold emotional and financial harm. People have begun trolling her on various social media accounts and she lost her job after her employer stated that he didn't want to be "associated" with someone that had her condition.*

On the advice of a friend, Sarah found a lawyer who filed suit in State C, claiming injuries based on Unrepresented's improper use of data. However, Unrepresented filed a choice of law motion arguing that because of language in its terms and conditions,[5] *West Virginia law should apply. The motion was successful, and the company, invoking a certain affirmative defense from a West Virginia statute that Sarah had never heard of, successfully claimed that they were immune from liability. As a result, the judge threw the case out.*

Why would a non-West Virginia company want data privacy issues to be handled under the laws of West Virginia? Because in <u>this</u> West Virginia, the bill

---

[3] Think of your favorite West Coast state that has sunny coasts and deep blue waters . . . . . and has as their black letter law the (Second) Restatement of Conflicts and the (Second) Restatement of Contracts.

[4] In this world, Unrepresented has issued Sarah a privacy notice that says, among other things, "we will not use any information you post in private groups in any way shape or form." The privacy notice also refers back to Unrepresented's terms and conditions as providing the "governing law, in the event of a breach."

[5] Unrepresented's terms and conditions included language stating, "This Agreement will be governed in accordance with the laws of the State of West Virginia."

"Safe Harbor for Cybersecurity Programs" was passed by the state governor instead of vetoed.[6] *As a result, the company relied on the law to successfully get the lawsuit thrown out on the grounds that the company had complied with the required safe harbor provisions and, as such, is completely immune to any suit related to data privacy harms, regardless of whether those harms were intentional or not.*

*****

There has been an uptick in the creation and passage of data privacy laws at the state level in the United States. In 2024, that pace accelerated. As of October 2024, over a dozen states had enacted comprehensive data privacy laws[7] with several others introducing bills in their last session, including West Virginia.[8]

Specifically, in its 2024 regular session, the West Virginia legislature: introduced, revised, and then passed a bill on this issue.[9] However, the changes from the bill between its introduction and its passage were so significant that the law itself was renamed to reflect this. When introduced, the bill was entitled the West Virginia Consumer Data Protection Act ("WVCDPA").[10] In contrast, the final bill was called the Safe Harbor for Cyber Security Programs Act.[11]

The changes were not just semantics.

The cybersecurity language that survived in the final bill was originally part of the WVCDPA, a law that was designed to protect consumers from data privacy harms. As such, the corporate *safe harbor* was created specifically as part of the *protections* that were being given within this consumer protection paradigm. However, when the final bill was passed, only the safe harbor remained.

This safe harbor, now untethered from the specific protections it was designed to mitigate, had the potential to take on an outsized role in data privacy litigation. Specifically, the revised bill could be read to provide an expansive, complete liability shield to *any* corporation that created data privacy harms to *any* consumer, *anywhere*, so long as the corporation simply changes its terms and conditions to require any suits related to data privacy be litigated under West Virginia law.

Luckily, the final bill, after having been passed by both the House of Delegates and the Senate in West Virginia, was subsequently vetoed by

---

6 *See* discussion, *infra* Section I.B.

7 *See* International Association of Privacy Professionals list, here for a compilation of all enacted laws in the United States.

8 H.B. 5338, 86th Leg., 2024 Reg. Sess. (2024 W. Va.), discussed *infra* in Section I.

9 *Id.*

10 H.B. 5338, Introduced Bill.

11 H.B. 5338, Enrolled Bill.

Governor Jim Justice and, thus never became law.[12] But, an analysis of the proposed safe harbor within the context of conflict of laws doctrine and potential corporate behavior shows us just how close to the precipice consumers—not just in West Virginia but across the country—actually came to this potential reality, and the consequences, likely unintended, that could have resulted.

As such, this essay proceeds as follows. Section I provides an overview of the data privacy law both as introduced (when it was the WVCDPA) and as passed (when it became something else entirely) during West Virginia's 2024 regular session. Specifically, in this Section, we provide a textual comparison between the law as introduced and the final bill that was passed to show how the cybersecurity safeguards—when untethered from consumer protections—had the power to provide expansive and unanticipated consequences.

In Section II we discuss the potential corporate response to the final bill. Specifically, we analyze how the law—when combined with intentional corporate action and doctrine regarding "choice of law"[13] principles and how they apply—could have had the unintended effect of creating blanket immunity for corporations so long as they updated their terms and conditions appropriately. In this Section we also (briefly) explore the harms and consequences that may have resulted both to West Virginians and people across the country. Here, we argue that if not for the Governor's veto, the results—however unintended—could have been significant, not just for consumers across the country but also for West Virginia itself.

As states continue to grapple with the issue of data privacy—we hope that this essay serves as a cautionary tale—regarding the delicate balance that must be achieved amongst data privacy laws, consumer protections, and corporate actions.

I. WHAT'S AT STAKE—A BIRD'S EYE VIEW OF WEST VIRGINIA'S 2024 BILL[14]

House Bill 5338—the 2024 West Virginia bill related to data privacy—was not the first time that the West Virginia legislature had grappled with this issue. In fact, West Virginia—like every other state in the nation—has a law on the books that requires companies to notify consumers if it has experienced a

---

[12] *See* Caity Coyne, "Justice Vetoed Eight Bills Passed by Legislatures this Session. Here's What they Would Have Done," W. VA. WATCH (Mar. 28, 2024, 8:27 PM), watch.com/2024/03/28/justice-vetoed-eight-bills-passed-by-legislators-this-session-heres-what-they-would-have-done/ (discussing H.B. 5338 and the Governor's reason for the veto).

[13] A choice of law provision is a standard clause in most commercial contracts and, more recently, in the terms and conditions of a website browser, that allows a particular party (in this case, the company that hosts the social media site) to apply the law from a state of their choice. *See* discussion *infra* Section II.A.

[14] For a comprehensive, side-by-side analysis of the introduced bill compared to the enrolled bill *see* Martin, *supra* note 1, at 118–122.

data breach. In addition, the state legislature, in its 2021 and 2022 session, unsuccessfully attempted to pass comprehensive data privacy laws.[15]
However, House Bill 5338 is distinguishable from its predecessors for two important reasons. First, this was the closest that this issue has come to actually becoming law in West Virginia; if not for a veto by Governor, the bill would have gone into effect. Second, the *changes* in the bill—between its introduction and its final passage—were *so significant* that the final bill could no longer accurately be named a consumer protection bill, instead becoming a safe harbor protection for companies. Unfortunately, a close analysis of the two bills shows that the safe harbor protections go beyond what the legislatures likely intended when the final bill was passed. Specifically, since the final enrolled bill in no way discusses its scope, in theory, any corporation can take advantage of the affirmative defense even when the person who is harmed is not a West Virginia citizen or resident. So, in our hypothetical, once Sarah's lawsuit is transferred to West Virginia, a company can invoke the affirmative defense as it was embodied in the enrolled bill and have her case dismissed. This marks a significant step back in protecting the privacy of consumers. As noted in *Data Privacy issues in West Virginia: An Overview*, West Virginians already possessed Article 6 claims in the data breach context.[16] Sarah, West Virginia consumers, and consumers nationwide would experience a significant reduction in those privacy rights.

When seen in the light of this hypothetical exercise, the consequences for West Virginia are significant indeed. Specifically, the safe harbor provisions, now de-coupled from the robust protections in the introduced bill instead become groundwork for blanket immunity for any company that wants to avail themselves of its protections, even if the company *intentionally* engaged in data privacy harms. To demonstrate how, in this Section we provide an analysis of each before comparing the similarities and differences between the two.

A. The Bill as Introduced[17]

Sometimes, the title of a bill can say a lot about its intent.[18] From the start, the original bill situated itself as a bill to minimize harms and provide

---

[15] For a comprehensive review of the 2021 Bill 3159 see Harrison Enright, Note, *What a Data Privacy Law Should Like in West Virginia: Balancing Competing Interests of Consumers and Businesses*, 125 W. VA. L. REV. 263, 286–290 (2022).

[16] Jena Martin, *Data Privacy in West Virginia: An Overview*, 124 W.VA. L. REV. ONLINE 1, 15 (2021) (noting "[a] case theory for data privacy violations based on the West Virginia UDAP has been advanced in both federal courts and tested in West Virginia state courts").

[17] The introduced bill would have amended the West Virginia Code in various places, most notably Chapter 31 (related to banks and banking) and Chapter 46A (West Virginia's Consumer and Credit Protection Act). Notably, the final bill that was passed would have only amended the Chapter 31 of the Code. *See infra* Section I.B.

[18] *See, e.g.*, The Connecticut Data Privacy Act, the Delaware Personal Data Privacy Act, and the Indiana Consumer Data Protection Act. For a full list of the national data privacy landscape, see *Which States Have Consumer Data Privacy Laws?*, BL (Sept. 10, 2024),

protections against data privacy violations. The title, "the West Virginia Consumer Data Protection Act," made that declaration clear.[19]

The rest of the introduced bill follows through on the promise contained in the title. For instance, after providing definitions, the bill begins with a discussion of affirmative defenses that a company can employ to reduce or prevent its liability under the Act. Specifically, the introduced bill provides that a covered entity that would like to avail itself of an affirmative defense under the Act, "shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of both personal information and restricted information."[20] Although the bill began with affirmative defenses, (rather than with a company's duties or a consumer's enumerated rights)[21] this alone would not change the consumer protection paradigm of the bill. Rather, these affirmative defenses, when combined with the protective-oriented language found later in the bill, could be seen as providing an incentive for corporations to install rigorous cybersecurity frameworks to ensure that data privacy harms are minimized. In addition, in order for a company to avail itself of the affirmative defense in the introduced bill, the design of its program must do *all* of the following:

> (1) Continually evaluate and mitigate any reasonably anticipated internal or external threats or hazards that could lead to a data breach.
> (2) Periodically evaluate no less than annually the maximum probable loss attainable from a data breach.
> (3) Communicate to any affected parties the extent of any risk posed and any actions the affected parties could take to reduce any damages if a data breach is known to have occurred.[22]

However, even within the parameters of consumer protection, the introduced bill had its limits. Crucially, the introduced bill placed a limitation on

---

https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws.

[19] The title also recalls other consumer protection laws. *See, e.g.*, the California Consumer Protection Act (the "CCPA"), the Virginia Consumer Data Privacy Act (the "VCDPA"), and the New Hampshire Privacy Act. *See id.*

[20] *See* H.B. 5338, 86th Leg., 2024 Reg. Sess. (2024 W. Va.), Introduced Bill.

[21] In doing so, the legislature may have been signaling a more business friendly stance than other jurisdictions. *Compare, e.g.*, H.B. 5338 *with* the CCPA, *supra* note 18 (beginning the law with the specific duties of a corporation); the Colorado Privacy Act (beginning their law with a declaration stating "the people of Colorado regard their privacy as a fundamental right and an essential element of their individual freedom.").

[22] H.B. 5338, Introduced Bill, §31A-8H-3, however, provides alternate ways that a company can "reasonably conform" to the cybersecurity framework.

a private right of action "with respect to any act or practices regulated therein."[23] Nonetheless, the subsequent language of the bill seemed able to provide relief. For instance, the law would have given West Virginia consumers key rights, provided regulation by West Virginia's Attorney General, and established a Fund where harmed consumers could potentially find relief.[24]

Unfortunately, the final bill had none of those things.

B. The Bill as Enacted[25]

The final bill is decidedly shorter than the introduced bill. That's because the final bill deletes all references to consumer protections that would have modified Chapter 46A of the West Virginia Code.[26] Instead, the final bill that passed the legislature focused *exclusively* on the affirmative defenses that a company could assert if it complied with a cybersecurity framework. Moreover, the language of the affirmative defense threshold (within the context of the cybersecurity framework) changed between the introduced and enrolled bill—in effect making it significantly easier to meet the threshold necessary to activate the affirmative defense.

From the first, the final bill signals to its readers that it is no longer a consumer data privacy act, aligned with other state's data privacy laws. Gone in the title is any mention of "consumer protection." Instead, the final bill carried the title "Safe Harbor for Cyber Security Programs." Following that pattern, the final bill adopts many of the same definitions as its earlier counterpart and, makes affirmative defenses the second point within the potential law—but with a lower threshold of compliance.

Recall, for instance, that the introduced bill required companies to engage with all three standards to avail itself of the affirmative defenses. In contrast, the final bill's affirmative defense only requires corporations to do *one* of the following:

> (1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of personal information and that reasonable [sic] conforms to an industry recognized cybersecurity framework, as described in §31A-8H-3; **or**
> (2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an

---

23 *Id.*

24 *Id*. In that sense, the introduced bill was aligned with other states' data privacy laws. *See* Martin, *supra* note 1.

25 H.B. 5338, Enrolled Bill.

26 West Virginia's data breach notification law is embedded within Chapter 46A.

> industry recognized cybersecurity framework, as described in §31A-8H3.[27]

However, while the changes to the affirmative defense are significant, the most consequential impacts of the would-be law stem from what was removed rather than what was added. Specifically, with *all* of the consumer protection language stripped from the final bill, only the definitions, the affirmative defenses, and the limitation on private rights of action remained.

Restructured in this way, the potential implications are troubling. Because, if companies still have the *protections* of affirmative defenses but no commiserate *obligations* to consumer protection then what would the affirmative defense language have protected these companies against? Our concern is that the answer might be *any* cause of action that implicates data privacy harms in West Virginia. This might especially prove true in light of the fact that the enrolled bill limits private rights of action related to these issues. Therefore, with no other "protections" within the law, a court could potentially find that affirmative defenses, now untethered from other key provisions of the law, would provide sweeping protections for data privacy harms. This specific concern—regarding the potential protection of intentional harms—was the reasoning behind Governor Jim Justice's veto.[28] As such, the final bill never became law.

But what if it had? This is question we explore in Section II, below.[29]

II. POTENTIAL RESPONSES AND THEIR EXPANSIVE EFFECTS

Corporations have a significant amount of flexibility regarding where they can be sued and, to some extent, what law would apply. As we discuss below, language that corporations use in their terms and conditions notices[30] can have significant effects on consumers' protections.

---

27 H.B. 5338, Enrolled bill (emphasis added).

28 The final bill was vetoed by Governor Jim Justice on March 27, 2024, preventing the bill from taking effect. In vetoing the bill, Governor Justice noted that while the bill was "well-intentioned . . . the final language in the bill created unintended consequences which require a veto of this legislation." Governor's Veto Message for H.B. 5338, Letter from Jim Justice, Governor of West Virginia, to Mac Warner, West Virginia Secretary of State (Mar. 27, 2024), https://www.wvlegislature.gov/Bill_Text_HTML/2024_SESSIONS/rs/veto_messages/HB5338.pdf. For instance, Governor Justice noted that "the potential for bad actors to abuse this law and to harm our citizens is unfortunately real." *Id.*

29 We would note that this is not just an academic exercise. Given that data privacy laws have been introduced in two of the last four years in West Virginia, we believe that there is a strong likelihood that the law will return. *See* Martin, *supra* note 1, at 21.

30 That boilerplate that most consumers mechanically scroll through and accept without reading. *See* Martin, *supra* note 1.

A. The Toll of Terms and Conditions

There are a lot of legal consequences bound within the language of terms and conditions. The "boilerplate" found within these clauses can implicate everything from what type of mechanism can be used to resolve a dispute (with several companies choosing binding arbitration); to what forum the suit can be brought; and most significant here, which state's law will apply.

Sarah S., our hypothetical plaintiff, could argue that clicking "I Agree" to the barely read terms on a site does not make an enforceable agreement, but, assuming the business set up its agreement correctly, Sarah could likely lose. Although these notices would likely all be categorized as "contracts of adhesion,"[31] the law may still enforce these agreements if there is some "manifestation of assent."[32]

In the context of traditional contract law, manifestation of assent can be made through words or conduct.[33] Electronic contracts are created in a plethora of ways, including electronic signatures, click-to-agree (clickwraps), sign-in wrap, and browsewrap agreements, many of which depend on user-conduct to indicate agreement.[34] Clickwrap contracts are some of the most enforceable, as long as it is clear that (1) an agreement is being made and (2) there is a way for the user to access the terms of the agreement.

In the hypothetical agreement above, assent appears to be straightforward. Because Sarah "clicked" on the agreement prompt to continue onto the site, that is likely enough to show sufficient conduct that manifests assent. The law is clear that "the conduct of a party may manifest assent even though he does not in fact assent."[35] As such, if the terms of the agreement were easily viewable, and it was clear from the text on the button when she was creating her account that Sarah was indicating to Unrepresented that she was agreeing to something, then the terms will likely apply even if Sarah didn't read it.[36]

---

[31] Although Sarah did not negotiate terms, it is unlikely the terms would be deemed exploitative by a court, and thus would still be enforceable. *See* Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999).

[32] RESTATEMENT (SECOND) OF CONTRACTS § 4 (AM. L. INST. 1981).

[33] *Id.* ("A promise may be stated in words either oral or written, or may be inferred wholly or partly from conduct.").

[34] *See* Martin, *supra* note 1.

[35] RESTATEMENT (SECOND) OF CONTRACTS § 19(3) (AM. L. INST. 1981), though this section also notes that a contract may be voidable due to "fraud, duress, mistake, or other invalidating cause."

[36] The structure of these terms and conditions also has implications in *this* universe, not just in our alternative world. For instance, Facebook and other real-world social media venues regularly update their terms of service and have mechanisms to notify existing users that changes have been made. In most cases, the remedy for users who do not want to agree with a site's terms of use is to stop using the website. *See*, *e.g.*, Facebook Terms of Service, stating:

B. Choose Wisely—The Impact of Choice of Law Norms

In contrast to the forum selection clauses, in order for a company to apply the law of a certain state, the law may require more than a notice embedded in the terms of a clickwrap agreement. For instance, under principles of *lex loci delicti*, and *lex loci injuria*, the law to be applied could be tied to either the site of the wrongdoing (*delicti*) or where the harm occurred (*injuria*). While this may seem a simple matter in situations where both the wrongdoing and the harm occurred in the same defined place (such as a pedestrian who is hit by a car in West Virginia), the matter can easily become more complicated in this modern, interconnected world. So, returning to Sarah (from our hypothetical) the questions that a court may have to confront are substantial, and may include (1) where should we determine the wrongdoing? (2) did the harm occur when Sarah discovered the postings? (3) did the harm occur, where the data servers were located?[37] In addition, depending on whether the cause of action was pled as a tort, a property issue,[38] or a breach of contract claim, the choice of law norms vary greatly.

Crucially, if Sarah were to plead her claim as a breach of contract issue,[39] Unrepresented could likely claim that West Virginia law applies, even though neither Sarah nor Unrepresented have any contacts with the state. How? Because, under some legal theories (as embodied in the Restatement (Second) of Conflict of Laws) the language of the contract could trump all other analyses.[40] And, since the language of this contract specifies West Virginia law, there is a real likelihood that West Virginia law could apply.[41] Keep in mind, this conceptual framework is specifically within claims that sound in contract. Should Sarah

---

> [W]e will notify you before we make changes to these Terms and give you an opportunity to review them before they go into effect. Once any updated Terms are in effect, you will be bound by them if you continue to use our Products. [. . .] if you do not agree to our updated Terms and no longer want to be a part of the Facebook community, you can delete your account at any time.

Section 4, FACEBOOK, https://www.facebook.com/terms.php.

[37] In fact, many companies strategically consider where to place their data servers (the machines that collect the information stored in the "cloud") precisely because of the potential impact of that venue's law. *See, e.g.*, Bill Ide, Google Moves its Services from China to Hong Kong, VOICE OF AMERICA (Mar. 21, 2010, 8:00 PM), https://www.voanews.com/a/google-to-redirect-chinese-services-through-hong-kong-88852572/114498.html (discussing Google's decision to move its servers from China in order to be outside the ambit of Chinese law related to censorship).

[38] For a discussion of property norms in this context, see Adam MacLeod, *Cyber Trespass and Property Concepts*, 10 IP THEORY 1 (2021).

[39] Not surprisingly, we have styled the facts in our hypothetical in a way that would support this—recall that Unrepresented stated that it would not disclose any information stated by users in private groups and then did exactly that in breach of their privacy policy and their general terms and conditions.

[40] RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187(1) (AM. L. INST. 1971).

[41] *Id.*

plead her case as a tort, a host of different rules would apply. For instance, courts have looked at the place where a company has the most significant contacts.[42]

Importantly, states with comprehensive data privacy laws have a greater chance of protecting their residents from a scenario like this one, assuming a company meets the threshold requirements to be covered by the law. As an example, the California Consumer Privacy Act ("CCPA") includes a clause that prohibits waiver of a consumer's data privacy protections.[43] While the choice of West Virginia governing law in the provisions of a contract would not be an explicit waiver of CCPA protections, it could serve as a *prospective* waiver since it could deprive a California resident of their state's statutory protections.[44]

C. A Note on the Expansive Effects of Unintended Consequences

The hypothetical we have laid out here is, by its nature, an extreme example of how the passage of H.B. 5338 could affect consumers from around the country—especially if their claim is pled as a breach of contract claim. However, we exhort readers to not lose sight of this crucial point: this bill, at a minimum, could harm West Virginians who are the victims of data privacy harms.[45] Moreover, it is easy to grapple with other scenarios that could unspool unintended consequences even further. Say for instance, companies examining this issue decided that that the promise of complete immunity from all claims was a significant enough boon to their bottom line that it was worth them establishing some presence in the Mountain State. So, these companies begin buying and building on acres of West Virginia land in order to create data farms where they would house their servers (and thereby strengthen their contacts with the state).[46] However, data centers require an incredible amount of land and other

---

[42] For one discussion of personal jurisdiction related to the many companies that host data on servers and the jurisdictional implications, *see* Damon Andrews & John Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313 (2013).

[43] California Consumer Privacy Act of 2018 §1798.192.

> Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.

Id.

[44] Gibbs v. Haynes Invs., L.L.C., 967 F.3d 332 (4th Cir. 2020). Arbitration agreements governed by tribal law would have kept plaintiffs from leveraging federal statutory protections and remedies: "we agree that the choice-of-law clauses amount to a prospective waiver such that the arbitration agreements [. . .] are unenforceable." *Id.* at 345.

[45] Because the plaintiffs in this case would be West Virginians, courts would be even more likely to allow both the forum and the body of law to be West Virginia. *See* discussion Section II.

[46] Andrews, *supra* note 42.

resources (such as water)[47] and, given West Virginia's relative abundance of both, it seems only a matter of time until corporations will consistently turn to West Virginia as a placement of their servers,[48] especially if the laws are particularly favorable here.

While, at first glance, this may seem like a potential benefit to the host jurisdiction, lessons drawn from human rights law would seem to indicate that, in fact, these "race to the bottom"[49] moves never serve the people of the state well.[50] In light of West Virginia's history as what some have dubbed an "internal colony,"[51] the likelihood that a corporation will use the state in ways that do not actually benefit their residents is all too real.

CONCLUSION

At their heart, corporations are profit-maximization entities. Therefore, if a particular jurisdiction holds the potential for large-scale immunity from suit around a specific issue, it seems likely that the corporation will find some way to take advantage of this. Unfortunately, rarely in this calculus does the corporation meaningfully weigh the externalities of its decisions, particularly as

---

47 *See* Caroline O'Donovan, *Fighting Back Against Data Centers, One Small Town at a Time*, THE WASH. POST (Oct. 5, 2024), https://www.washingtonpost.com/technology/2024/10/05/data-center-protest-community-resistance/.

48 In fact, it's already begun. *See* Dan Swinhoe, *1GW Hydrogen-Powered Data Center Campus Proposed in West Virginia*, DATA CTR. DYNAMICS (Aug. 17, 2023) https://www.datacenterdynamics.com/en/news/1gw-hydrogen-powered-data-center-campus-proposed-in-west-virginia/ (stating that "Texas-based Fidelis New Energy . . . this week announced that it had selected Mason County West Virginia as the location for a hydrogen production facility and data center campus.").

49 We borrow the term "race to the bottom" from other fields, including business and human rights discussions. In that context, the race to the bottom signifies the lengths that countries will go to in order to secure, for instance, foreign direct investments from powerful corporations; usually by minimizing legal regulations that would have protected affected communities and individuals. For a discussion of the phenomenon see Steven Ramirez, *The End of Corporate Governance Law: Optimizing Regulatory Structures for a Race to the Top*, 24 YALE J. REG. 313 (2007).

50 West Virginia, in particular, has bared the brunt of many of the efforts of corporations to use its resources, leading commentators to describe the state as a colony and one subject to the "resource curse"—where those locales with the greatest resources are often subject to the worst harms. *See* Jena Martin & Karon Powell, *Parallel Worlds: Comparing Rural Development to Development in Global Communities*, 120 W. VA. L. REV. 1107 (2018).

51 Shaun Slifer, *1,500,000 Gas Masks: Appalachia as a Resource Colony in Rod Harless & Dan Culter's* The Hillbillys: A Book for Children, VIEWPOINT MAG. (Apr. 8, 2022), https://viewpointmag.com/2022/04/08/the-hillbillys-a-book-for-children-early-1970s/. Although, Slifer acknowledges the complicated choice in naming Appalachia as an internal colony, we, like he, feel that "the colony model still appeals on the ground as an organizing concept today . . . it is a useful shorthand which helps to crystallize *how it feels to live* in the rural parts of the region for many people today." *Id.*

it applies to potential victims of their acts. However, these decisions often come with very real harms that can befall the people who use their services. As such, it is imperative that the legislatures (who are tasked with protecting their constituents) take up the mantle and consider *all* of the consequences that may come from such an expansive law as H.B. 5338.

Too much is at stake to do otherwise.