Perspectives from FSF Scholars
March 16, 2021
Vol. 16, No. 14

Inconsistent State Data Privacy Laws Increase Confusion and Costs

by

Andrew Long *

I. Introduction and Summary

Following California's lead, and within the void created by the failure of Congress to pass preempting federal legislation, an increasing number of states have proposed their own comprehensive data privacy regimes. Virginia Governor Ralph Northam just signed the Consumer Data Protection Act into law. Other states where bills have been introduced include Florida, Minnesota, New York, Oklahoma, and Washington State. When the California Consumer Privacy Act (CCPA) went into effect at the beginning of 2020, businesses rationally chose to apply its provisions nationwide rather than attempt to identify, and treat differently, California residents. Now, the adoption of rival state data privacy laws similarly might drive companies to abide a Frankenstein's monster assembled from the most onerous privacy regulatory requirements. Counterproductive consumer confusion, along with unreasonably burdensome and unjustifiably costly compliance obligations, inevitably would result.

By design, Internet traffic recognizes no political boundaries, national or international. A single set of data privacy rules therefore should govern throughout the United States. Members of Congress from both parties appear to acknowledge the wisdom of a national regime. Likewise, there seems to be widespread support for constructive best practices that include: an opt-out

approach for non-sensitive personal information; fact-specific, case-by-case inquiries; enforcement by the Federal Trade Commission and state attorneys general; and evenhanded treatment of all with access to consumer data, regardless of outdated regulatory classifications. But fundamental disagreements on at least two key issues – preemption of state laws and the availability of a private right of action – thus far have stood in the way.

A private right of action in the privacy context would lead to undesired outcomes: a disproportionate impact on small and nascent competitors; inconsistent, jurisdiction-bound holdings; inadequate remedies for affected consumers; and inappropriate incentives for members of the plaintiffs' bar to pursue lawsuits, in particular class actions. Regrettably, some of the state laws under consideration, including those in Florida, Minnesota, and New York, do provide for a private right of action. And with regard to the need for federal preemption, a state-by-state approach, left unchecked, will render effective compliance all but impossible, leave consumers uncertain as to their rights, and disproportionately impact small and upstart companies.

Already in 2021, multiple states are considering their own versions of comprehensive data privacy legislation. This threatens to exacerbate the current situation, in which California, rather than Congress, effectively has defined a single set of rules of the road, and could lead to multiple, inconsistent approaches. While the bills thus far introduced – and, in the case of Virginia, recently signed into law by the Governor – share many similarities, on the margins there are meaningful distinctions. These variations underscore the practical challenges that both consumers and businesses would face under a balkanized approach – not to mention the resulting costs that necessarily and unreasonably would be imposed – and highlight why a preempting federal data privacy law is essential.

Commenters – and I include myself among them – have described a scenario where multiple states adopt differentiated data privacy laws as a "patchwork." But given the inherent nature of Internet traffic, a more likely outcome is one in which expediency and a need to minimize compliance costs motivate businesses to assemble and abide by a nationwide, worst-of-all-worlds collection of the most onerous obligations imposed by state laws. The broadest definition of a covered entity from State A. The widest set of privacy rights from State B. The most extreme data minimization obligations from State C. And so on.

Although conceivably more easily administrable, such a worst-of-all-worlds approach would be more restrictive and costly than what is required by any one state. We saw similar corporate behavior after the CCPA went into effect at the beginning of last year: companies chose to comply with its provisions nationally rather than take on the risk associated with attempts to identify which of their customers are and are not California residents. If more states regulate data privacy, that challenge will become far greater, by an order of magnitude. Especially for small and up-and-coming businesses that lack the legal and administrative resources of established players.

Of course, consumers, too, will suffer. Businesses – in particular large, entrenched rivals – have the financial wherewithal to hire lawyers and consultants to monitor legislative efforts in all fifty states, compile a comprehensive list of obligations, and craft effective compliance programs. But how are individuals to comprehend both what their state of residence requires and what each company in fact is doing? Not every company will come up with an identical set of

requirements, and some likely will attempt to comply with the laws of each state, within that state. The result will be mass confusion on the part of consumers.

When California passed the CCPA, many expressed optimism that it would prompt Congress to adopt preemptive federal legislation. That, sadly, has not yet come to pass. But with more states considering data privacy rules, the pressure steadily rises. Congress should enact a law that recognizes the value of ad-supported services; ensures consumers are well informed and afforded reasonable rights with respect to their personal information; empowers the FTC with exclusive federal enforcement authority; rejects a private right of action; and preempts rival state laws.

II. Overview of Proposed State Data Privacy Laws

California's CCPA became the default data privacy law of the land at the beginning of 2020.[1] In the November election, state voters approved the California Privacy Rights Act (CPRA), commonly referred to as the CCPA version 2.0, the major provisions of which will go into effect on January 1, 2023.[2] In addition, Governor Ralph Northam days ago signed the Virginia Consumer Data Protection Act (VCDPA).[3] Other states in which data privacy laws have been proposed include Florida, Minnesota, New York, Oklahoma, and Washington State. In New York alone, over fifty pieces of privacy legislation so far have been introduced.[4]

What follows is a high-level overview of key provisions in those bills under current consideration.

Virginia: Virginia just became the second state to pass a comprehensive data privacy law.[5] The VCDPA will become effective on the same day as the CPRA: January 1, 2023.[6] As I described in a February 5, 2021, post to the *FSF Blog*,[7] the VCDPA establishes consumer rights to access, amend, and delete collected personal data; a right to data portability; and the right to opt-out of the sale of personal data to third parties, targeted advertising, and profiling.[8] It also defines a subcategory of personal information, "sensitive data," for which opt-in consent is required.[9] It exclusively authorizes the state attorney general to enforce its provisions via civil actions,

---

[1] *See generally* Andrew Long, "California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019), available at https://freestatefoundation.org/wp-content/uploads/2019/10/California's-Heavy-Handed-Approach-to-Protecting-Consumer-Privacy-–-Exhibit-A-in-the-Case-for-Federal-Preemption-102819.pdf.

[2] *See generally* Andrew Long, "California Voters Approve the California Privacy Rights Act: A Detailed Analysis of Its Requirements and Impact," *Perspectives from FSF Scholars*, Vol. 15, No. 60 (November 17, 2020), available at https://freestatefoundation.org/wp-content/uploads/2020/11/California-Voters-Approve-the-California-Privacy-Rights-Act-111720.pdf.

[3] *See generally* "Consumer Data Protection Act," Virginia Senate Bill No. 1392, 2021 Session, available at https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf (*VCDPA*).

[4] *See* Lydia de la Torre and Ann J. LaFrance, "Off to the Races: Over 50 Privacy Bills Introduced in the State of New York," *The National Law Review* (February 24, 2021), available at https://www.natlawreview.com/article/to-races-over-50-privacy-bills-introduced-state-new-york.

[5] *See* Cat Zakrzewski, "Virginia governor signs nation's second state consumer privacy bill," *The Washington Post* (March 2, 2021), available at https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina/.

[6] *See VCDPA* § 3.

[7] *See* Andrew Long, "Virginia's Consumer Data Protection Act Soon Could Become Law," *FSF Blog* (February 5, 2021), available at https://freestatefoundation.blogspot.com/2021/02/virginias-consumer-data-protection-act.html.

[8] *See VCDPA* § 1 (creating Code of Virginia Chapter 52, § 59.1-573(A)).

[9] *See id*. (creating Code of Virginia Chapter 52, §§ 59.1-571, 59.1-574(A)(5)).

expressly declines to allow for a private right of action, and affords covered entities a 30-day cure period.[10]

Florida: House Bill (H.B.) 969, which enjoys the support of Florida Governor Ron DeSantis and House Speaker Chris Sprowls,[11] would create consumer rights to know, access, delete, correct, and opt-out of the sale of personal information to third parties.[12] Like California's CCPA, it would prohibit discrimination against a consumer for exercising his or her rights but allow a business to "offer a different price, rate, level or quality of goods and services to the consumer if the price or difference is directly related to the value provided to the business by the consumer's personal information."[13]

Significantly, H.B. 969 would impose data minimization obligations: covered entities must delete data "after satisfaction of the initial purpose for collecting or obtaining such information, or after the duration of a contract, or 1 year after the consumer's last interaction with the business, whichever comes first."[14]

H.B. 969 would establish a private right of action for:

> A consumer whose nonencrypted and nonredacted 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 an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information ….[15]

An aggrieved consumer could pursue both (1) statutory damages ranging from $100 to $750 per consumer per incident or actual damages, whichever is greater, and (2) injunctive or declaratory relief.[16]

More broadly, the bill would empower the Department of Legal Affairs to initiate a civil enforcement action after providing a 30-day cure period.[17]

---

[10] *See id*. (creating Code of Virginia Chapter 52, § 59.1-579) ("Nothing 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."). *See also id*. (creating Code of Virginia Chapter 52, § 59.1-580).
[11] *See* Leslie Postal, "DeSantis, GOP leaders push 'big tech' bill to beef up consumer privacy laws," *Orlando Sentinel* (February 15, 2021), available at https://www.orlandosentinel.com/news/education/os-ne-desantis-bill-privacy-protections-florida-20210215-oovsbzmuffhyhkavtbhhvsikma-story.html ("Gov. Ron DeSantis said Monday he will support legislation to 'check the growing power and influence of big tech' and give Florida consumers 'more control of their data.'").
[12] *See* Florida House Bill 969, 2021 Session, § 2 (creating Florida Statutes §§ 501.173(3)-(6)), available at https://www.flsenate.gov/Session/Bill/2021/969/BillText/Filed/PDF (*H.B. 969*).
[13] *See id*. § 2 (creating Florida Statutes § 501.173(7)).
[14] *See id*. (creating Florida Statutes § 501.173(2)(f)).
[15] *Id*. (creating Florida Statutes § 501.173(12)).
[16] *Id*.
[17] *Id*. (creating Florida Statutes § 501.173(13)).

In another recent post to the *FSF Blog*, I noted that, on March 10, 2021, H.B. 969 received unanimous approval from the Regulatory Reform Subcommittee upon its first reading.[18] If passed, which appears likely, it would go into effect on January 1, 2022.[19]

Minnesota: House File (H.F.) 36, under consideration in Minnesota, is similar in many respects to the Florida legislation discussed immediately above. It would provide consumers with the right to know, access, and delete collected personal information, the right to opt out of the sale of that data to third parties, and a right of nondiscrimination.[20]

However, the private right of action created by H.F. 36 would not be limited to data breaches: "any person injured by a violation of this chapter may bring a civil action to receive or recover" statutory damages between $100 and $750 "per consumer, per violation, or the consumer's actual damages, whichever is greater," as well as fees, other equitable relief, and exemplary damages "in the case of a willful and malicious violation."[21]

H.F. 36 would go into effect on June 30, 2022.[22]

New York: Identical to a bill introduced during the last legislative session, the New York Privacy Act, Assembly Bill A680 (NYPA), in a number of respects is far more intrusive than the state laws already passed in California and under consideration elsewhere.[23] By way of example, the NYPA would:

- Apply expansively to all "legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state" – that is, without reference to minimum annual gross revenues or numbers of consumers from whom personal data is collected, as is the case in most draft state laws;[24]
- Require that consumers give "express and documented consent" – in other words, opt in – before personal information can be used, processed, or shared;[25]
- Impose a "data fiduciary" obligation requiring covered entities to "exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk" and "act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances";[26]

---

[18] *See* Andrew Long, "Florida Vies for Bronze in Race to Create Patchwork of State Data Privacy Laws," *FSF Blog* (March 12, 2021), available at https://freestatefoundation.blogspot.com/2021/03/florida-vies-for-bronze-in-race-to.html.
[19] *H.B.* 969 § 3.
[20] *See* Minnesota H.F. No. 36, Ninety-Second Session, §§ 3-8, available at http://wdoc.house.leg.state.mn.us/leg/LS92/HF0036.0.pdf.
[21] *Id.* § 9, subdivision 1(b).
[22] *Id.* § 10.
[23] *See generally* "New York privacy act," New York Assembly Bill A680, 2021-2022 Regular Sessions, § 2 (adding a new Article 42, §§ 1100 *et seq*. to the New York Consolidated Laws, General Business Law (GBS)), available at https://legislation.nysenate.gov/pdf/bills/2021/A680 (*NYPA*).
[24] *NYPA* § 2 (creating GBS § 1101(1)).
[25] *Id.* (creating GBS §§ 1102(1), 1103).
[26] *Id.* (creating GBS § 1102(1)).

- Create consumer rights to access, correct, delete, and transfer personal information and prohibit profiling;[27] and
- Establish a private right of action.[28]

The NYPA would become effective a mere 180 days after passage.[29]

Oklahoma: The Oklahoma Computer Data Privacy Act (OCDPA) was introduced in the state House of Representatives at the beginning of February.[30] The OCDPA establishes consumer rights to know[31] and delete[32] collected personal information as well as a right to nondiscrimination.[33] It also: includes a lower revenue threshold – $10 million – for covered entities than many states;[34] requires opt-in consent for the collection and sale of personal information to third parties;[35] and creates a private right of action that includes statutory damages – $2,500 per violation, $7,500 if intentional – to be awarded in addition to actual damages.[36] Enforcement responsibilities otherwise are left to the Oklahoma Corporation Commission.[37]

If passed, the OCDPA would go into effect on November 1, 2021.[38]

Washington State: Lawmakers in Washington State have attempted to pass data privacy legislation on multiple occasions. The Washington Privacy Act of 2021, Senate Bill (SB) 5062 (WPA),[39] and the People's Privacy Act, House Bill (HB) 1433 (PPA),[40] constitute their latest efforts.

The WPA served as the model for Virginia's data privacy law, the VCDPA. It defines the following consumer privacy rights: access, correction, deletion, data portability, and nondiscrimination.[41] It also empowers consumers to opt out of the sale of their personal information to third parties, targeted advertising, and profiling.[42] It does not create a private right

---

[27] *Id*. (creating GBS § 1103).
[28] *See id*. (creating GBS § 1109(3)) ("In addition to any right of action granted to any governmental body pursuant to this section, any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions.").
[29] *See NYPA* § 3.
[30] *See generally* "Oklahoma Computer Data Privacy Act," 1st Session of the 58th Legislature, available at http://webserver1.lsb.state.ok.us/cf_pdf/2021-22 FLR/HFLR/HB1602 HFLR.PDF (*OCDPA*).
[31] *See id.* §§ 11, 13 (creating Oklahoma Statutes Title 17, §§ 901.11, 901.13).
[32] *See id.* § 12 (creating Oklahoma Statutes Title 17, § 901.12).
[33] *See id*. § 23 (creating Oklahoma Statutes Title 17, § 901.23).
[34] *See id*. § 3 (creating Oklahoma Statutes Title 17, § 901.3(A)(1)(d)(1)).
[35] *See id.* §§ 14, 17 (creating Oklahoma Statutes Title 17, §§ 901.14, 901.17).
[36] *See id*. § 27 (creating Oklahoma Statutes Title 17, § 901.27(C)).
[37] *See id*. (creating Oklahoma Statutes Title 17, § 901.27(B)).
[38] *See id*. § 30.
[39] *See generally* "Washington privacy act," Senate Bill 5062, 67th Legislature, available at http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate Bills/5062-S2.pdf?q=20210218100914 (*WPA*). The *WPA* also includes specific provisions relating to contact tracing and other data privacy concerns during the ongoing COVID-19 pandemic. *See WPA* Parts 2 and 3.
[40] *See generally* "People's privacy act," House Bill 1433, 67th Legislature, available at http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/House%20Bills/1433.pdf?q=20210302104029 (*PPA*).
[41] *See WPA* § 107(7).
[42] *See id*. § 103.

of action.[43] The state attorney general has exclusive enforcement authority and covered entities have 30 days to cure an alleged violation.[44]

The WPA was approved on a 48-1 vote by the state Senate on March 3, 2021.[45] If passed, it would go into effect on July 31, 2022.[46]

By contrast, the PPA, which is supported by the American Civil Liberties Union,[47] includes far more stringent requirements. By way of example, the PPA: requires that consumers opt in to the collection of their personal information[48] and reconfirm that consent annually;[49] imposes a one-year cap on data retention;[50] applies to a wider group of businesses;[51] and provides for a private right of action with both (1) liquidated damages up to $10,000 or actual damages, whichever is greater, and (2) punitive damages.[52] In enforcement actions brought by the state attorney general, a district attorney, or a city attorney, civil penalties "of up to $25,000 per violation or up to four percent of annual revenue of the covered entity, data processer, or third party, whichever is greater," may be imposed.[53]

III. Businesses Might Comply With the Most Onerous Requirements Imposed by the Various States, Leading to Consumer Confusion and Unjustified Costs

When California's CCPA went into effect at the beginning of 2020, businesses, including Microsoft,[54] chose to comply with California's data privacy rules throughout the United States.[55] Indeed, a survey conducted by the Interactive Advertising Bureau (IAB) revealed that:

---

[43] *See id*. § 111(1) ("A violation of this chapter may not serve as the basis for, or be subject to, a private right of action under this chapter or under any other law.").
[44] *See id*. § 112.
[45] *See* Jake Holland, "Washington State Inches Closer to Passing Consumer Privacy Law," *Bloomberg Law* (March 4, 2021), available at https://news.bloomberglaw.com/tech-and-telecom-law/washington-state-inches-closer-to-passing-consumer-privacy-law (noting that "[t]he state Senate has passed similar iterations of the bill two years in a row, but they have failed to garner enough support in the state House").
[46] *See id*. § 402.
[47] *See* ACLU Press Release, "Washington State Rep. Shelley Kloba Introduces New Data Privacy Bill: the People's Privacy Act" (January 28, 2021), available at https://www.aclu.org/press-releases/washington-state-rep-shelley-kloba-introduces-new-data-privacy-bill-peoples-privacy (revealing that "[t]he People's Privacy Act was created by the ACLU of Washington with input and support from the Tech Equity Coalition" and characterizing the bill as "a strong people-focused alternative to" the WPA).
[48] *See PPA* § 2(10) (announcing the legislative finding that "[r]equiring entities to obtain opt-in consent prior to the use or disclosure of personal information is essential to protecting personal privacy").
[49] *See id*. § 7(1).
[50] *See id*.
[51] *See id*. § 3(5) (setting the annual revenue threshold for a "covered entity" at just $10 million obtained through 300 or more transactions and the minimum number of consumers from whom personal information is collected at only 1,000).
[52] *See id*. § 10(1).
[53] *Id*. §§ (10)(2)(b)(ii), (10)(3)(b)(ii).
[54] *See* Julie Brill, "Microsoft will honor California's new privacy rights throughout the United States," *Microsoft on the Issues* (November 11, 2019), available at https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/ (announcing that Microsoft "will extend CCPA's core rights for people to control their data to all our customers in the U.S.").
[55] *See* Jeff John Roberts, "Here Comes America's First Privacy Law: What the CCPA Means for Business and Consumers," *Fortune* (September 13, 2019), available at https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/ (concluding that "since the data privacy law covers out-of-state merchants who sell to Californians – or even display a website in the state – the reality is that companies will comply with the CCPA,

> Approximately 60% of "businesses" make CCPA rights (e.g., access, deletion, sale opt-outs) available regardless of jurisdiction (i.e., whether in U.S., EU, LATAM, etc.). This trend may reflect that it can be easier to administer consumer rights uniformly, regardless of consumer location. It may also relieve "businesses" of any concern about differential treatment of their consumers."[56]

Presumably, such decisions hinged at least in part upon concerns regarding the ability to identify accurately which consumers were California residents. After all, neither billing nor mailing addresses necessarily nor infallibly reveal state of residence. Costs undoubtedly played a role, as well.

The same IAB survey summary referenced above indicates that "'[b]usinesses' that do restrict the opt-out right to certain jurisdictions typically rely on 'geofencing' (such as via IP lookup to detect whether a consumer is located in California)."[57] However, many of the state laws discussed in the previous section, as well as the CCPA itself, require merely that a consumer be a resident of that state – not that he or she be physically located therein at any specific point in time.[58] A traveling resident, therefore, would appear to pose a challenge to technical tools, such as geofencing, employed to ensure compliance.

As a consequence, and as the number of state laws increases, businesses subject to *any* data privacy law reasonably may elect to behave as though *all* such laws apply – and to *every* consumer, regardless of where they happen to be located at the time of any given interaction or the state indicated by the address they provide.

Out of such rational, and understandably risk-averse, compliance-related decisionmaking, a costly Frankenstein's monster of requirements might arise.

The following discussion does not attempt to accomplish the herculean task of assembling every single most-onerous provision from the proposed bills identified above. Instead, for purposes of illustration, it focuses only on a small sample of provisions. (Enough, I trust, for you to get a sense of the level of complexity and cost required to develop a comprehensive compliance program.) As you quickly will appreciate, the resulting compendium of worst-case scenarios logistically is unworkable. Any less-burdensome alternative, on the other hand, could lead to inadvertent violations.

As an initial matter, these bills establish different minimum thresholds – including annual gross revenue amounts and number of individuals, or individuals, households, and devices, subject to data collection – for a business to be deemed covered. A business that earns more than $25

---

rather than step away from the world's fifth largest economy. And rather than create separate systems, lawyers are in consensus that companies will just apply the CCPA nationwide").

[56] "IAB CCPA Benchmark Survey Summary" (November 2000), available at https://www.iab.com/wp-content/uploads/2020/11/IAB_CCPA_Benchmark_Survey_Summary_2020-11.pdf, at 6.

[57] *Id.*

[58] *See, e.g.*, VCDPA § 1 (creating Code of Virginia Chapter 52, § 59.1-5731) (defining a "consumer" as "a natural person who is a resident of the Commonwealth"); *NYPA* § 2 (creating GBS § 1100(3) (defining a "consumer" as "a natural person who is a New York resident").

million in annual gross revenues would be subject to Florida H.B. 969,[59] while a business that earns more than just $10 million would trigger Oklahoma's OCDPA[60] – and New York's NYPA defines no such minimum.[61] Similarly, Florida's H.B. 969 sets the bar at 50,000 consumers, households, or devices;[62] Virginia's VCDPA[63] and Washington State's WPA at 25,000 consumers;[64] and – once again – the NYPA includes no floor whatsoever. A business adopting a worst-of-all-worlds approach therefore might assume that all state data privacy laws apply regardless of annual earnings or number of consumers – or consumers, households, and devices – from whom it collects personal information.

While we are on the topic of the NYPA, businesses might also elect to apply its unprecedented and untested "data fiduciary" concept to every one of their customers.[65]

Returning the focus to the requirements themselves, different proposed state laws require businesses to respond to a verified consumer request – say, for a copy of all data collected from said consumer – within different amounts of time. For example, the OCDPA provides 45 days and up to a 90-day extension,[66] the VCDPA establishes a 45-day window and allows for a 45-day extension under certain circumstances,[67] and Florida's H.B. 969 draws the line at 45 days and just 30 days, respectively.[68] Businesses opting for a conservative approach might in all cases deny themselves any additional time beyond that allowed by the proposed Florida law.

Relatedly, some proposed state laws, such as Oklahoma's OCDPA, require businesses to provide free copies of the personal information collected once each year,[69] while others – including New York's NYPA[70] and Washington State's WPA[71] – require businesses to do so twice annually. Two times a year could become the rule nationwide.

On the topic of data minimization, some proposed state laws contain no such requirements, while Florida's H.B. 969 states that:

> A business shall provide and follow a retention schedule that prohibits the use and retention of personal information after satisfaction of the initial purpose for collecting or obtaining such information, or after the duration of a contract, or 1 year after the consumer's last interaction with the business, whichever occurs first.[72]

---

[59] *See H.B. 969* § 2 (creating Florida Statutes § 501.173(1)(e)(I)).
[60] *See OCDPA* § 3 (creating Oklahoma Statutes Title 17, § 901.3(A)(1)(d)(1)).
[61] *See NYPA* § 2 (creating GBS § 1101(1)) ("This article applies to legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state.").
[62] *See H.B. 969* § 2 (creating Florida Statutes § 501.173(1)(e)(II)).
[63] *See VCDPA* § 1 (creating Code of Virginia Chapter 52, § 59.1-572(A)).
[64] *See WPA* § 102(1)(b).
[65] *See NYPA* § 2 (creating GBS § 1102).
[66] *See OCDPA* § 21 (creating Oklahoma Statutes Title 17, § 901.21(B)).
[67] *See VCDPA* § 1 (creating Code of Virginia Chapter 52, § 59.1-573(B)(1)).
[68] *See H.B. 969* § 2 (creating Florida Statutes § 501.173(8)(b)).
[69] *See OCDPA* § 21 (creating Oklahoma Statutes Title 17, § 901.21(E)).
[70] *See NYPA* § 2 (creating GBS § 1103(1)).
[71] *See WPA* § 105(c).
[72] *H.B. 969* § 2 (creating Florida Statutes § 501.173(2)(f)).

Florida's proposed data minimization requirements could become the *de facto* federal standard.

This entire discussion, of course, leaves to the side the following fundamental issue: how businesses are to grapple with the reality that these proposed state laws define "personal information" in a multitude of different ways.

Residents of specific states travel throughout the country and access the Internet as they do. This renders efforts to determine with sufficient certainty when, and to whom, the data privacy rules of a given state should apply a high-risk – and expensive – endeavor. But as the examples above illustrate, attempts to make sure all bases are covered quickly would become unmanageable, even for well-resourced businesses. Individual consumers attempting to understand their rights, by contrast, would find themselves utterly overwhelmed.

IV. Conclusion

The disconnect grows between (1) the reality that the Internet knows no borders, and (2) efforts by political subdivisions – states – to impose their own regulatory preferences. California leads the way with both so-called network neutrality and data privacy laws.[73] The real possibility that other states may follow on both fronts is troubling.[74] We therefore continue to look to Congress for leadership on these important issues.

Absent a federal data privacy regime – one that ensures consumers understand how their personal information is used; establishes reasonable rights with respect to that information, including the right to opt out of its sale to third parties; provides for exclusive federal enforcement by the FTC; and, critically, preempts regulation by individual states – businesses may find no viable option but to abide a Frankenstein's monster composed of the most unfavorable provisions from the universe of state laws – and consumers will be left in the dark as to the rules of the road that apply. Such a result would be both unjustifiably costly and counterproductive.

* Andrew Long is a Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland.

Further Readings

"Florida Vies for Bronze in Race to Create Patchwork of State Data Privacy Laws," *FSF Blog* (March 12, 2021).

"Virginia's Consumer Data Protection Act Soon Could Become Law," *FSF Blog* (February 5, 2021).

---

[73] *See* Seth L. Cooper, "District Court Allows California's Net Neutrality Law to Go Forward," *FSF Blog* (February 26, 2021), available at https://freestatefoundation.blogspot.com/2021/02/district-court-allows-californias-net.html.

[74] *See, e.g.*, Casey Lide, "State Net Neutrality Laws May Lead to Federal Legislation," *The National Law Review* (March 1, 2021), available at https://www.natlawreview.com/article/state-net-neutrality-laws-may-lead-to-federal-legislation ("[B]roadband providers face the prospect of enforcement of California's law, as well as the emergence and enforcement of net neutrality laws in other states…. Faced with a patchwork of net neutrality rules, broadband trade associations may well conclude that a consistent set of rules is desirable.").

"California Voters Approve the California Privacy Rights Act: A Detailed Analysis of Its Requirements and Impact," *Perspectives from FSF Scholars*, Vol. 15, No. 60 (November 17, 2020).

"Proposed Revisions to California's Privacy Law Create Additional Unwanted Uncertainty, Underline Need for Federal Legislation" *FSF Blog* (October 23, 2020).

"California Privacy Regulation Must Account for the COVID-19 Crisis," *Perspectives from FSF Scholars*, Vol. 15, No. 26 (May 27, 2020).

"A Privacy Private Right of Action Is Inferior to FTC Enforcement," *Perspectives from FSF Scholars*, Vol. 15, No. 4 (January 21, 2020).

"Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," *Perspectives from FSF Scholars*, Vol. 14, No. 42 (December 4, 2019).

"California's Privacy Law: Recent Developments Underscore the Need for Preemptive Federal Law," *FSF Blog* (November 21, 2019).

"California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019).