Managing Compliance with the Growing Patchwork of State Privacy Laws

By: Phil Yannella, Kim Phan and Greg Szewczyk[1]

I. Introduction

Over the past four years, U.S. companies have been forced to expand their compliance programs to comply with an expanding array of international and U.S. state privacy laws. The wave of privacy laws began in May 2018, when the General Data Protection Regulation (GDPR) became effective, triggering new compliance obligations for U.S. companies with operations in the European Union. On the heels of the GDPR, other countries such as Brazil, Australia, India, Canada and China passed or expanded new privacy legislation, further expanding the scope of privacy compliance for U.S. multinationals.

In the U.S., there has likewise been a creeping expansion of state privacy laws. In 2020, the California Consumer Privacy Act (CCPA) became effective, triggering new legal requirements for U.S. companies that conduct business in California and generate yearly revenues of greater than $25,000,000.[2] Other states, such as Nevada, Utah, and Maine, have since passed smaller less comprehensive privacy laws.

In November 2020, California voters approved via ballot initiative, the California Privacy Rights Act (CPRA), which significantly expands on the CCPA and introduced a number of

---

[1] **Philip N. Yannella** is the Practice Leader of Ballard Spahr 's Privacy & Data Security Group and the firm's Cybersecurity Incident Response Team. He provides clients with 360-degree advice on the transfer, storage, and use of digital information.

Kim Phan is a Partner at Ballard Spahr, who counsels clients on federal and state privacy and data security laws and regulations. Her work in this area encompasses strategic planning for companies to incorporate privacy and data security considerations throughout product development, marketing and implementation.

Greg Szewczyk is a Partner in Ballard Spahr's Privacy and Data Security and Litigation groups. He has represented companies in cases in numerous privacy and cybersecurity contexts, including data breach class actions, post-incident business-to-business disputes, and alleged violations of laws for online tracking practices.

[2] Cal. Civ. Code § 1798.140(d).

GDPR-like privacy concepts as well as some entirely new legal obligations. In March 2021, the Virginia legislature passed the Virginia Consumer Data Protection Act (VCDPA)[3], which incorporates many of the same concepts as the CPRA, but varies in enough ways that compliance with the CPRA does not necessarily entail compliance with the CPRA.

At the same time, numerous other states have proposed, but ultimately failed to pass state privacy laws. Recently, proposed privacy laws in Florida[4] and Washington[5], for example, failed to pass. The Washington Privacy Act (WPA) has now failed three consecutive years, foundering on the issue of a private right of action – a common point of disagreement in many state legislatures. Presently, other proposed state privacy laws, such as bills in New York and Connecticut, remain alive and could potentially become law in 2021. Due in part to a lack of a federal privacy law – various proposals continue to stalldue to disagreements over enforcement and pre-emption – it is very likely that U.S. states will continue to propose and consider privacy legislation after 2021.

The dilemma for U.S. multinationals is how to manage compliance with the growing patchwork of state and international privacy obligations. These laws, as discussed in more detail in this article, share many characteristics but they each differ in ways that complicate compliance. If privacy law was a Venn diagram, the GDPR would form the outermost ring, with the CPRA, CCPA, and VCDPA fitting within the GDPR in loosely concentric circles. But there is enough variance between these laws that simply complying with the GDPR would not be sufficient for companies subject to all these laws.

The purpose of this article is to compare and contrast the major U.S. privacy laws, identifying areas of overlap as well as areas where compliance will require state-specific analysis, disclosures and policies

II. Status and Timeline of U.S. State Privacy Legislation and Laws

---

3 Va. S.B. 1392, § 59-572(A).

4 HB 969 (proposed Florida Privacy Protection Act).

5 S.B. 5062 (Washington Privacy Act).

Since November 2020, two U.S. states – California and Virginia -- have passed comprehensive privacy legislation. The new California law, the CPRA, is essentially a redline and expansion of the CCPA, and will become effective in January 2023. In July 2021, the California Privacy Protection Agency – a first of its kind state privacy regulator created by the CPRA – will announce formal rule making for CPRA regulations.[6] These regulations are expected to be finalized by July 2022. The CPPA will commence enforcement of the CPRA in July 2023. [7]

Virginia's privacy law, the VCDPA, will become effective in January 2023.[8] Unlike the CPRA, however, there is no provision for rule-making in Virginia.

As has become a yearly pattern, numerous other states proposed privacy legislation in 2021, but presently none have passed. Proposed legislation in Alabama, Arizona, Colorado, Connecticut, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, and New York is still under consideration. Legislatures failed to pass proposed privacy legislation in Mississippi, Oklahoma, Florida, Washington, and Utah.

III. Comparing Different State Approaches to Key Privacy Issues

A. Compliance Thresholds

Generally speaking, state privacy laws apply to entities that collect personal information from a state's residents in connection with their business operations, plus the satisfaction of certain qualifying thresholds. One of the key differences between state privacy laws and legislation is what thresholds must be met in order for the laws to apply.

Under the CCPA, those thresholds are set forth in the definition of "business." [9] The CCPA defines business to mean virtually any for-profit entity, including any "sole

---

6 Cal. Civ. Code § 1798.185(d).

7 *Id.*

8 Va. S.B.1392, § 59-572(A)

9 Cal. Civ. Code §1798.140(c)

proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners."[10]

Business is further defined to mean any such entity that "collects consumers' personal information or on the behalf of which that information is collected, and that alone, or jointly with others, determines the purposes and means of processing of consumers' personal information, that does business in the State of California." The CCPA does not define what it means to "do business" in the state.

In addition to the above, an entity is only a "business" under the CCPA if it satisfies one or more of the following thresholds:

A. Has annual gross revenues in excess of $25 million;

B. Alone or in combination buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California consumers, households, or devices; or

C. Derives 50 percent or more of its annual revenues from selling California residents' personal information.[11]

The CPRA follows the CCPA's model, but it makes important changes that will impact which businesses are subject to the law. The $25 million threshold is the same, but the CPRA specifies that it is measured by the preceding calendar year.[12] The second threshold was changed to 100,000 or more Californian consumers or households (but not devices), and only for those whose personal information is bought, sold, or shared (as opposed to received for a business purpose).[13] The third threshold remains the same.

---

[10] *Id.*

[11] *Id.*

[12] Cal. Civ. Code §1798.140(d).

[13] *Id.*

The VCDPA, using the terminology from the European GDPR, governs the conduct of "controllers" rather than businesses.[14] A controller is defined to mean "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[15] The applicability thresholds are set forth in a specific section dedicated to the scope of the law, which provides that the VCDPA applies to "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that"

i. During a calendar year, control or process personal data of at least 100,000 consumers (defined to mean a resident of Virginia); or

ii. Control or process personal data of at least 25,000 Virginia consumers and derive over 50 percent of gross revenue from the sale of personal data. [16]

As "process" is defined to mean any operation or set of operations performed on personal data, the first threshold is broader than the CPRA in scope.[17] The second prong's percentage threshold is tied sales of all personal data, and not just sales of Virginia residents. [18] However, the 25,000 component is designed to ensure a certain level of minimum contacts with the state. There is no revenue threshold under the VCDPA.

Other states have generally followed these two models, but with important nuances. For example, the proposed Colorado Privacy Act generally follows the VCDPA model, applying to "controllers" that (i) process the personal data of 100,000 Colorado residents during a calendar year, or (ii) control or process the personal data of 25,000 Colorado residents and derive any revenue from the sale of data.

---

[14] The VCDPA also uses the GDPR's term "personal data" rather than the CPRA's "personal information."

[15] Va. S.B. 1392, § 59.1-571.

[16] § 59.1-572(A).

[17] § 59.1-571.

[18] *Id.*

The proposed Florida Privacy Protection Act (FPPA) has switched between the two models—whereas the initial bill introduced in the House followed the CCPA model fairly closed, the version that passed the Senate closely resembles the VCDPA.[19]

It is widely expected that several more states will continue to propose, advance, and pass privacy legislation. Especially with respect to applicability thresholds, the model chosen will be very significant: under the California model, larger companies that do business nationally will likely be subject under the annual revenue threshold, whereas under the Virginia model, such companies may not be subject if they do not have a significant presence in that state. In the media context, this difference could be particularly significant when serving a relatively small number of consumers outside of the state of primary broadcast or publication.

B. **Exclusions and Exemptions to Compliance**

Differences in the substance and scope of exclusions will also play a significant role in whether or how state privacy laws apply. For example, the CCPA and CPRA exclude personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act ("GLBA").[20] GLBA-regulated financial institutions therefore do not have to comply with the CCPA and CPRA for personal information regulated by the GLBA, but they do have to comply with the CCPA and CPRA for other sets of personal data.

Complying with these different standards for different data can obviously cause operational difficulties. The VCDPA, on the other hand, provides full exclusions for financial institutions subject to the GLBA.[21] Differences in the scope and extent of exclusions relating to HIPAA and the FCRA will be similarly important in those industries.

Four types of exclusions are likely to have significant impacts on the media industry: (1) exclusions for business-to-business data; (2) exclusions for employees; (3) exclusions relating to publicly available information; and (4) exclusions for non-profit organizations.

---

[19] Although both the Florida House and Senate passed competing versions of this bill, the two chambers were unable to reach consensus on a final bill before the close of the legislative session on April 30, 2021.

[20] Cal. Civ. Code §1798.145

[21] Va. S.B. 1392, § 59.1-572(B).

The CCPA, the CPRA, and the VCDPA all provide exclusions for personal information collected and processed in the business-to-business context. The VCDPA accomplishes this exclusion through its definition of "consumer," which "does not include a natural person acting in a commercial or employment context."[22] The CCPA and CPRA accomplish it through exemption provisions, which are currently set to expire on January 1, 2023, although it is widely believed that the provisions will be extended and/or renewed.[23]

With respect to employee personal information, the VCDPA provides a full exclusion through its definition of "consumer," whereas the CCPA and CPRA provided limited exclusions that still require businesses to provide some notices to employees, job applicants, contractors, officers, and directors. As with the business-to-business exclusion, the CPRA employee exclusion is set to expire but is expected to be extended.

The different treatment that may be afforded to publicly available information is another area that may be of particular importance to media companies. For example, under the CPRA, personal information is defined to exclude "consumer information that is . . . [p]ublicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions."[24] "Publicly available" is defined to include information that is lawfully made available to the general public "from a widely distributed media."[25] The Florida bill contains a similar provision. The VCDPA defines "sale of personal data" to exclude "[t]he disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience."[26] Nuances in factual scenarios may have important consequences, so media companies should take particular care in analyzing the impact of how personal information is collected in the newsgathering process.

---

22 § 59.1-571 (defining consumer)

23 Cal. Civ. Code §1798.145.

24 Cal. Civ. Code § 1798.140(v)(2).

25 *Id.*

26 Va. S.B. 1392, § 59.1-571

Finally, all of the privacy laws that have passed to date have excluded non-profit organizations from their scope.[27] However, non-profit media organizations should not assume this will be the case for all future bills, as the proposed Washington Privacy Act[28]—which failed to advance in recent weeks—would have applied to non-profits starting in 2026. Accordingly, it is important for non-profit media organizations to stay apprised of state privacy laws, and potentially begin building compliance regimes in some areas of their operations.

C. Data Minimization Principles

While much of the available guidance had already suggested that organizations minimize the data they collect and store, the new privacy laws impose statutory obligations on subject companies to minimize data collection and use.

For example, the CPRA provides that a "business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected."[29] The VCDPA provides that a controller 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" and prohibits businesses from processing personal data "for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed."[30]

Media companies and digital platforms/technology companies should begin considering and adopting policies to allow compliance with these requirements, including analyzing the scope of the business purpose for which personal data is collected. For example, when collecting personal data as part of the newsgathering process, the company may wish to specify whether such data is being collected and processed solely with respect to that story, or whether it is collected and processed for a broader substantive issue that may allow broader use.

D. Data Protection and Privacy Risk Assessments

---

[27] § 59.1-572(B); Cal. Civ. Code, § 1798.140(d).

[28] S.B. 5062 (Washington Privacy Act)

[29] Cal. Civ. Code § 1798.100(c).

[30] Va. S.B. 1392, § 59.1-574.A.1-2.

Many companies are already performing data security risk assessments on an annual basis. However, the new privacy laws may impose an obligation to incorporate privacy risk assessments into a company's procedures—including with specific criteria in a written document that is discoverable by state regulators. For organizations that are not subject to the European GDPR, the privacy assessment requirements may be a new concept.

Under the CPRA, businesses whose processing presents a significant risk to consumers' privacy or security will be required to (1) conduct an annual cybersecurity audit, and (2) submit to the newly formed California Privacy Protection Agency a risk assessment with respect to their processing of personal information.[31] The CPRA does not specifically define what constitutes a significant risk, but it does state that factors to be considered include the size and complexity of the business and the nature and scope of processing activities.

The risk assessment must weigh the benefits of processing to the business, consumers, other stakeholders, and the general public, against the potential risks to the rights of the consumers.[32] This balancing must be done with the goal of restricting or prohibiting the processing if the risks to the privacy of the consumer outweigh the benefits. The risk assessment must be provided to the newly formed Agency "on a regular basis."[33] The new Agency will be issuing regulations, so businesses will likely gain better clarity on the frequency and substantive requirements of the privacy risk assessment. [34]

Under the VCDPA, all controllers are obligated to perform and document a data protection assessment for each of five identified processing activities: (1) processing for targeted advertising; (2) processing for sales; (3) processing for profiling where there are specific types of foreseeable risks; (4) processing sensitive data; and (5) processing that involves personal data that presents a heightened risk of harm.[35] The data protection assessment must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller,

---

31 Cal. Civ. Code § 1798.185(a)(15).

32 *Id.*

33 *Id.*

34 *Id.*

35 Va. S.B. 1392, § 59.1-576

the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. [36]

The VCDPA provides that the Attorney General can request, pursuant to an investigative civil demand, that a controller disclose any data protection assessment that is relevant to an investigation, and the controller must make the data protection assessment available.[37] However, the VCDPA specifically provides that any disclosed data protection assessment will not be subject to public inspection under the Virginia Freedom of Information Act, and that production does not waive any applicable attorney-client privilege or work product protection.[38]

E. Enforcement and Civil Liability

One of the most important differences in state privacy laws is whether there is a private right of action. Indeed, one of the most common reasons why proposed state privacy laws have failed to pass is because of a failure to arrive at a consensus with regard to a private right of action.

The CCPA, which will remain in effect until January 2023, when the CPRA becomes effective, has a private right of action.[39] Plaintiffs have the right to collect the greater of actual damages or between $100 and $750 in statutory damages, per consumer per incident. The CPRA continues the CCPA's private right of action with statutory damages for data breaches caused by a business's failure to maintain reasonable security measures. The VCDPA expressly states that it does not create a private right of action.[40]

The CPRA will be enforced by the newly created California Privacy Protection Agency, which will have the ability to seek $2,500 per violation, or $7,500 for intentional violations or violations involving minors.[41] The Agency will be able to do so in administrative actions.

---

36 *Id.*

37 *Id.*

38 *Id.*

39 Cal. Civ. Code § 1798.150.

40 Va. S.B. 1392, § 59.1-579, 580.

41 Cal. Civ. Code § 1798.199.90

The VCDPA will be enforced by the Virginia Attorney General, who will be able to seek up to $7,500 per violation, plus reasonable expenses and attorneys' fees.[42]

The key issue likely to determine whether more states pass privacy laws is the degree to which state legislatures are able to arrive at a consensus with regard to the private right of action.

F. Consumer Disclosures

Transparency has long been an essential principle to the protection of consumer privacy. The CCPA requires that a company with an online privacy policy must include a description of consumer privacy rights, a list of the categories of personal information it has collected about consumers in the preceding 12 months, and if applicable, a list of the categories of personal information it has sold or disclosed about consumers in the preceding 12 months. [43] In addition to prescribing the content of these consumer disclosures, the CCPA regulations also require that any consumer disclosures be in easy-to-read plain language, formatted to draw consumer attention, be displayed in the same language as a company's marketing materials, be accessible to those with a disability, and be provided in a clear and conspicuous manner whether presented online or offline.[44]

Similarly, the VCDPA requires that companies provide consumers with a privacy notice that must include the categories of personal data processed by the controller, the purpose for processing personal data, how consumers may exercise their consumer rights, the categories of personal data that the controller shares with third parties, the categories of third parties with whom the controller shares personal data, and whether a controller sells personal data to third parties or processes personal data for targeted advertising.[45]

G. Consumer Rights

---

42 Va. S.B. 1392, § 59.1-579, 580.

43 Cal. Civ. Code § 1798.199.90

44 CCPA Reg. § 999.304(a), 308.

45 Va. S.B. 1392, § 59.1-574(C).

The ability for consumers to exercise some level of control over the collection, use, and sharing of their personal information has been embodied in state privacy laws as various consumer rights. As observed in California, Virginia, and in the various state privacy legislative proposals that have been introduced so far in 2021, these consumer rights generally fall into the following broad categories:

- Right to Access (know what personal information a company has collected)
- Right to Correct (direct a company to resolve inaccuracies in personal information)
- Right to Delete (direct a company to permanently destroy personal information)
- Right to Restrict Use (limit the ability of a company to use personal information)
- Right to Portability (transfer of personal information to another party)[46]

State privacy laws generally require that companies provide consumers with easily accessible means to exercise these consumer rights, subject to verifying and/or authenticating the identity of the consumer making the request.

H. Vendor Obligations

Vendors often have access to the personal information of consumers in their role providing various services to companies. Thus, state privacy laws have extended consumer privacy protections to these third parties. Some states, like Virginia, have modeled these third-party requirements in a manner similar to the GDPR by designating an entity as a "controller" or a "processor."[47] Other states are following the standard set by the CCPA and designated an entity as a "business" or a "service provider."[48] Regardless of the terminology, it is clear that

[46] Va. S.B. 1392, § 59.1-573; Cal. Civ. Code § 1798.110-121.

[47] Va. S.B. 1392, § 59.1-575.

[48] Cal. Civ. Code § 1798.110-40(v),(w).

states intend to impose privacy obligations to downstream recipients of consumer personal information.

The CPRA requires that prior to sharing any consumer personal information, a business must enter into a written contract with a service provider that:

- Specifies the limited and specified purpose for selling/disclosing personal information;
- Requires the same level of privacy protection as those imposed on the business;
- Grants the business audit rights on any downstream uses of personal information by the service provider;
- Requires the service provider to provide notification to the business if the service provider can no longer comply with CPRA; and
- Grants the business the authority to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information by the service provider.[49]

Similarly, under the VCDPA, a controller must enter into a written contract with any third-party processors that set forth:

- Instructions for processing personal information;
- The nature and purpose of any personal information processing;
- Types of personal information that will be subject to processing;
- The duration of any processing;
- Subject to a duty of confidentiality, an obligation to delete or return personal information when the relationship between the controller and processor terminates; and

[49] § 1798.100(d).

- An affirmative obligation to provide necessary information as part of any data protection assessments being conducted in compliance with the VCDPA.[50]

Due to the lengthy amount of time required to negotiate and finalize amendments to vendor agreements, companies should be planning ahead to incorporate these new contract clauses in a timely manner ahead of the January 1, 2023 effective date for both the CPRA and the VCDPA.

I. Financial Incentives

As previously discussed above, state privacy laws prohibit companies from discriminating against or otherwise penalizing consumers who choose to exercise their privacy rights. Such discrimination could take any one of the following forms:

- Denying goods or services to the consumers;
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- Providing a different level or quality of goods or services to the consumers; or
- Suggesting that the consumers will receive a different price or rate for goods or services or a different level or quality of goods or services.

However, financial incentives or other benefits can be provided to consumers without violating this prohibition, subject to certain conditions. In California, businesses must provide consumers with a notice of financial incentive that describes the material terms of any financial incentive program so that a consumer may make an informed decision about whether to participate. [51] Consumers must provide opt in consent to any such financial incentive program and must be able to withdraw from the program at any time.[52] The CCPA regulations also

---

50 Va. S.B. 1392, § 59.1-575.

51 Cal. Civ. Code § 1798.125(b).

52 *Id.*

require that any notice of financial incentive explain how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data.[53] The CCPA prohibits any financial incentive that would be unjust, unreasonable, coercive, or usurious.

The CPRA states that, "Consumers should benefit from businesses' use of their personal information" and expressly contemplates financial incentive programs like loyalty, rewards, discount, or club card programs.[54] VCDPA does not set forth the detailed requirements of the CCPA, but Virginia does require voluntary participation to opt in to such programs.[55] As other states enact privacy laws, the various requirements associated with financial incentive programs may vary, but it seems clear that a path forward for these types of programs will likely be incorporated into any new state laws.

J. Opt Outs and Consents

One of the most complicated areas of privacy compliance relates to management of differing state requirements for opt-outs and consents for the sale or sharing of personal information. The CCPA requires an opt-out for the "sale" of personal information.[56] The CPRA expands this right and includes a required consumer opt-out for the "sharing" of personal

---

53 The CCPA regulations provide the following examples of how a business can calculate the value of consumer data: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data. (2) The average value to the business of the sale, collection, or deletion of a consumer's data. (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers. (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information. (5) Expenses related to the sale, collection, or retention of consumers' personal information. (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference. (7) Profit generated by the business from sale, collection, or retention of consumers' personal information. (8) Any other practical and reasonably reliable method of calculation used in good faith.

54 Cal. Civ. Code § 1798.125(b).

55 Va. S.B. 1392, § 59.1-574(A)(4).

56 Cal. Civ. Code § 1798.120.

information.[57] The CPRA also provides consumers with a limited right to opt out of the processing of "sensitive personal information."[58]

Virginia similarly requires an opt-out for the sale of personal information as well as the sharing of personal information for "targeted advertising." Virginia, unlike California, requires a consumer consent for the processing of "sensitive personal information."

The reason compliance with these opt-out and consent rules is so complicated lies in the different definition of key terms such as "sensitive personal information," "sale", and "targeted advertising."

1. Definition of Sale

The CPRA adopts the CCPA's definition of sale, which requires the sharing of personal information to a third party for monetary "or other valuable consideration". What "valuable consideration" means is not defined under either law and has been a source of significant legal debate under the CCPA, particularly in the context of behavioral advertising. Virginia, by contrast, defines sale exclusively to require monetary consideration.

As with other areas of privacy law, California's and Virginia's approach toward the definition of sale have become the dominant models for other proposed privacy laws. The WPA and the FPPA – both of which failed this year – follow the California model. Nevada, by contrast, follows the Virginia model.

2. Definition of Sensitive Personal Information

The CPRA (but not the CCPA) provides consumers with a limited right to opt-out of the processing of sensitive personal information.[59] The limited nature of the right may explain the law's very long list of what constitutes sensitive information, which includes "social security number, driver's license number, state identification number, passport, financial account number, credit card number, precise geolocation, racial and ethnic information, religious or philosophical

---

57 *Id.*

58 § 1798.121.

59 *Id.*

belief, union membership, genetic data, the contents of text or email messages unless read by the intended recipient, biometric data, sexual orientation or sex life."[60]

By contrast, Virginia's privacy law requires affirmative consent prior to the processing sensitive personal information, but defines the term much more narrowly. Under the VDCPA, sensitive personal information is race/ethnic information, religious affiliation, medical diagnosis, genetic data, biometric data precise geolocation, personal information of a minor, sexual orientation, citizenship or immigration status. [61] It remains to be seen how much of an operational impact these new consent requirements will be for media companies and digital platforms/technology companies subject to the VDCPA because, with the exception of precise geolocation, most of the data defined as sensitive would not be automatically collected by websites or apps but would typically require the completion of forms or surveys, which often include express consents already.

3. The Definition of Consent

One area of commonality among recently passed, as well as proposed but defeated, privacy laws is the definition of consent. Both the CPRA and the VDCPA define consent to require affirmative actions.[62] The CPRA definition of consent is as follows: "'Consent means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through dark patterns does not constitute consent."[63]

---

60 § 1798.140(ae).

61 Va. S.B. 1392, § 59.1-571.

62 The WPA and FPPA included similar definitions of "consent."

63 Cal. Civ. Code, § 1798.140(h).

The requirement of affirmative action to signal consent is similar to the GDPR, and stands in stark contrast to other U.S. privacy laws, such as the TCPA or the Wiretap Act, which allow consent to be implied by consumer conduct. The CPRA's reference to dark patterns reflects growing regulatory concern with the use of deceptive interfaces to manipulate consent. What "dark patterns" means is not currently defined, and bears close monitoring.

4. Definition of Targeted Advertising

The CPRA expands on the CCPA by providing consumers with a new opt-out for the sharing of personal information. "Sharing", however, is defined to refer to sharing for the purposes of "cross contextual behavioral advertising"[64], which is further defined to mean "the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[65]

The VDCPA similarly provides an opt-out for targeted ads, but defines "targeted advertising" to mean the display advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests." [66]Notably the definition does not include contextual ads, first-party ads, consumer's request for information or feedback or the processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

Even before the passage of these laws, adtech models were in a state of flux with Google moving away from allowing tracking cookies, and Apple requiring that app developers obtain consent prior to enabling tracking on applications available through the Apple Store. What adtech models will rise in place of the tracking cookie, and whether those models will fall within the definition of targeted advertising is an issue U.S. companies will need to carefully monitor.

5. *Automated Profiling*

---

64 § 1798.140(ah).

65 § 1798.140(k).

66 Va. S.B. 1392, § 59.1-571.

Another area of commonality among the CPRA and the VDCPA (as well as other proposed, but defeated U.S. state privacy laws) is with regard to automated profiling. This is yet another concept borrowed from the GDPR, and is intended to protect consumers from the potential downside of algorithmic profiling.

Both the CPRA and VCDPA laws define "profiling" to cover any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[67] The VDSPA provides an opt-out for profiling that has a "legal effect."[68] What "legal effect" means is not defined under the law, and bears close monitoring by U.S. companies. The CPRA expressly delegates rule-making to the CPPA to address profiling of consumers.[69]

IV. Recommendations for Managing Compliance

How then should U.S. companies, particularly media companies and digital platforms/technology companies , that may be subject to multiple overlapping privacy laws manage compliance?

As an initial matter, companies should determine what laws actually apply to them. There are differing thresholds for compliance under the Virginia and California laws (to say nothing of the GDPR). Assuming a company hits a threshold trigger for compliance, the next question is the extent to which the company can avail itself of exclusions, particularly exclusions for employees and B2B transactions. After scoping the areas of data subject to privacy laws, companies should next determine the extent to which their obligations will vary under applicable laws. For example, an opt-out may be required in California but not Virginia for the same kind of processing activity. The answer to this question then raises another question: should companies strive for compliance with the most restrictive law where privacy laws overlap or address compliance at the state level?

---

67 Va. S.B. 1392, § 59.1-571; Cal. Civ. Code § 1798.140(z)

68 Va. S.B. 1392, § 59.1-573(A)(5).

69 Cal. Civ. Code § 1798.185(C)(16)

Some of the core compliance projects that companies may need to pursue include (1) data mapping – in particular mapping sharing activities, profiling, high risk activities, and characterizing vendors; (2) revising record retention programs to address new data minimization requirements; (3) revising vendor contracts; (4) assessing opt-out and consent requirements, which maybe a very granular analysis; and (5) assessing the extent to which the company can avail itself of any legal exemptions from privacy obligations.

Issues that companies should continue to monitor include: the status of rule-making in California – which is likely to significantly impact operations decisions – likely revisions to the VCDPA; the passage of additional state privacy laws; changes in behavioral advertising models that may or may not trigger the need for opt-outs; and the adoption at the corporate level of new automated technologies involving consumer data that may constitute profiling.