

DATA PRIVACY'S PATCHWORK EXPANDS

In Colorado, just when it appeared that efforts to pass data privacy legislation would go on hiatus, a successful last-minute push enabled it to become the second state this year, and third overall, to enact comprehensive privacy legislation.

The Colorado Privacy Act (CPA) adds to myriad sector-specific regulations and anticipates additional regulations aimed at cybersecurity. While it is similar to Virginia and California's data privacy statutes, there are some distinct differences, and since other states will likely follow suit, organizations may need to consider a patchwork approach.

BROADER OPT-OUT AND ENFORCEMENT POWERS

The consumer opt-out right under the CPA is different from California and Virginia. By 2024, companies must allow consumers to opt out through a global privacy control browser, rather than on a website-by-website basis. While the details of this global browser setting have not been determined and will be specified by the Colorado Attorney General (AG) by July 2023, companies must allow consumers across all websites to opt out of data processing that involves the sale of personal data, targeted advertising or profiling.

Enforcement is also slightly different under the CPA. In addition to the AG, any of the state's 22 district attorneys can bring an enforcement action, a first in privacy legislation in the U.S. If enforcement ensues, the CPA includes a 60-day cure period for companies to bring their practices in line with the CPA's requirements.

RESTRICTED USE OF 'DARK PATTERNS' AND DATA

The CPA is also the first statute to explicitly prohibit obtaining consumer consent through the use of dark patterns. Dark patterns – which manipulate users of websites and apps into doing things they did not intend – often implicate data collection and consumer consent, and thus have become a recent focus of regulators.

The Federal Trade Commission (FTC) and California AG have both taken action to address dark patterns this year, the FTC through a workshop hosted in April and California through modification of the CCPA's regulations. Colorado's

PEOPLE

F. Scott Galt, CIPP/E

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

inclusion of this provision in its legislation could signal the start of a trend.

Controllers under the CPA are also subject to a few unique requirements, including the requirement to minimize the use of personal data by limiting the collection of personal data to what is adequate, necessary and relevant to the specified purpose.

SIMILARITIES BETWEEN CPA AND EXISTING REGULATIONS

Organizations attempting to comply with the CPA can take comfort in knowing a lot of it is borrowed from existing regulations. For example, the rights to access, review and correct data are similar to the California Consumer Privacy Act (CCPA), Consumer Data Protection Act (CDPA) in Virginia, Global Data Protection Regulation (GDPR) in Europe, and various sector-specific laws. Like the CCPA, CDPA and GDPR, companies are also required to enter into written agreements with third parties, vendors and service providers that process data on their behalf.

The CPA's consumer notice requirements are also similar to other legislative frameworks. Under the CPA, companies must maintain a privacy notice that describes the categories of data collected, the purposes for which data is processed, how and where consumers may exercise their rights, and the categories of third parties with whom data is shared, among other things.

The CPA's applicability and scope are also limited in ways similar to the CDPA. For example, under both the CPA and CDPA, the definition of a "consumer" does not encompass individuals acting in a commercial or employment context, job applicants, or beneficiaries of individuals acting in an employment context.

SUMMARY OF CURRENT STATE LEGISLATION

The table below contains an overview of some of the key differences between the legislation in Colorado, Virginia and California:

	Colorado (CPA)	Virginia (CPDA)	California (CCPA)
Effective Date	July 2023	January 2023	January 2020 (will be replaced by CPRA in 2023)
Companies	Companies that meet	Companies that meet either of the following: - control or process the	Companies that meet any of the following: - gross annual revenue



Subject to the Law	<p>either of the following:</p> <ul style="list-style-type: none">- collect and store the personal data of more than 100,000 consumer s; or- derive revenue from the sale of personal data of at least 25,000 consumer s <p>Nonprofit entities that meet the above thresholds are subject to the requireme nts.</p>	<p>data of at least 100,000 consumers; or</p> <ul style="list-style-type: none">- companies that control or process the data of at least 25,000 consumers and derive 50% of its revenue from the sale of personal data <p>Nonprofit entities are exempt.</p>	<p>of more than \$25 million;</p> <ul style="list-style-type: none">- buy, receive or sell the personal data of more than 50,000 California residents; or- derive more than 50% of their revenue from selling personal data <p>Nonprofit entities are exempt.</p>
-----------------------------------	--	--	--



Special Requirem ents for Sensitive Data?	Yes	Yes	No
Consumer Opt-Out Rights?	Yes – compliance with a universal opt-out through a global privacy control browser setting required by July 2024	Yes – on a website- by-website basis	Yes – on a website- by-website basis
Purpose /Process ing Limitati ons	Yes	Yes	Yes
Require s a Risk Assessm ent or Data Protecti	Yes – for certain processi ng activities	Yes – for certain processing activities	No



on Assessm ent?			
Special Require ments for Youth Data?	No	Yes – opt-in required if under 13	Yes – opt-in required if under 16

AT's Privacy and Data Security practice has vast experience navigating all aspects of the complex data privacy regulatory scheme and regularly counsels clients – whether business-to-business, direct-to-consumer, e-commerce, or anything in between – across a variety of sectors on data privacy obligations. For more information specific to your business needs, please contact one of the authors or your regular AT attorney.