KILPATRICK TOWNSEND

Compliance Amid Disorder: How to Comply with the Growing Patchwork of State and Local Privacy Laws

John Brigagliano

Associate | Technology, Privacy and Cybersecurity

E-mail:
jbrigagliano@kilpatricktownsend.com

Laura Gardner

Senior Corporate Counsel | Microsoft

E-mail:
laura.gardner@microsoft.com

Jason Loring

Chief Privacy and Security Counsel | EY

E-mail:
jason.m.loring@ey.com

Amanda Witt

Partner | Technology, Privacy and Cybersecurity

E-mail:
awitt@kilptratricktownsend.com

Roadmap

- New State Laws Effective in 2023
- Interoperability - GDPR vs. US State Privacy Laws
- How to Manage a Privacy Program
- Other Legal Considerations – AI, Data Brokers and Biometrics
- Potential Proposed State Legislation

KILPATRICK TOWNSEND

California Privacy Rights Act (CPRA)

CPRA Timeline and Intro

- On November 3, 2020, California voters passed Proposition 24, the California Privacy Rights Act ("**CPRA**").
- Additional rounds of regulations from the AG's office with regards to the CCPA.
- CPRA will become effective on January 1, 2023 with enforcement set for July 1, 2023.
- Significant rulemaking under the law is required to be finalized by July 1, 2022, but that deadline will be missed.
- The California AG has generally taken a cooperative approach to enforcement, but that remains uncertain under the CPRA

Steps to Take Now to Prepare

- Review data maps or conduct data mapping to determine if the organization processes **sensitive personal information** and for what purposes. Develop a plan for making the personal information non-sensitive.
- If the organization has a launched a **"Do Not Sell"** button, determine if the functionality covers sharing
- Identify **retention periods** for personal information collected from consumers, and decide whether those retention periods should be reconsidered before making the periods publicly available.

Steps to Take Now to Prepare (cont'd)

- Outline a process for consumers to **correct personal information**, including verification.
- For **service providers under the CCPA**, evaluate whether CPRA restrictions on service providers prohibit the organization from continuing to act as a service provider.
- Explore enhancing **email security practices** such as to require multifactor authentication and increase the frequency of mandatory password changes.

The CDPA goes into effect January 1, 2023.

Virginia CDPA Overview

- Applies to anyone that conducts business in the Commonwealth and either
  - Controls or processes the personal data of at least 100,000 consumers or
  - Derives more than 50% of its gross revenue from the sale or processing data belonging to at least 25,000 consumers.
- No private right of action
- 30 day cure period
- $7500 per violation fine + injunctive relief + attorney's fees
- Increased consumer rights akin to GDPR/CPA/CPRA

Virginia CDPA Rights

- **Right to Access**
- **Right to Correct**
- **Right to Delete**
- **Right to Data Portability**
- **Right to Opt Out** of processing personal data for the purposes of targeted advertising, the sale of personal data and profiling
- **Right to Appeal**
- **Opt-in Consent is Required for Collecting Sensitive Information (Includes Location Information & Biometrics)**

The CPA goes into effect <u>July 1, 2023</u>.

Colorado CPA Overview

- Applies to businesses that:
  - Control or process the personal data of 100,000 Colorado consumers per year; or
  - Derive revenue or receive a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 Colorado consumers
- No private right of action
- 60 day cure period; expires January 1, 2025
- Up to $20,000 fines per violation
- Increased consumer rights akin to GDPR/CDPA

Colorado CPA Rights

- **Right to Access**
- **Right to Correct**
- **Right to Delete**
- **Right to Data Portability**
- **Right to Opt-Out** of processing of personal data concerning the consumer for purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer
- **Right to Appeal**
- **Opt-in Consent is Required for Collecting Sensitive Data (Includes Biometrics)**

The Utah CPA goes into effect <u>December 31, 2023</u>.

Utah Consumer Privacy Act (CPA) Overview

- Applies to a business that conducts business in UT/targets UT consumers, has annual revenues of $25 million or more and:
  - Controls or processes the personal data of 100,000 Utah consumers per year; or
  - Derives over 50% of its revenue from the sale of personal data and processes or controls the personal data of 25,000 Utah consumers
- No private right of action
- Excludes employee and B2B personal data
- 30 day cure period that does not sunset
- Up to $7,500 fines per violation & exclusively enforced by AG
- Increased consumer rights akin to GDPR/CDPA

Utah CPA Consumer Rights

- **Right to Confirm PD is being processed**
- **Right to Access**
- **Right to Delete**
- **Right to Obtain a Copy / Portability**
- **Right to Opt-Out** of processing of personal data for targeted advertising and the sale of personal data
- **For Sensitive Data (Includes Biometrics)**, must first provide notice and give opportunity to opt out

	CO CPA	CDPA	CCPA, as amended by the CPRA	GDPR
Right to opt-out of sale	✓	✓	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-in	Opt-in	Opt-out	Opt-in
Statutory cure period for violations	✓	✓	✗	✗
Right to appeal denials of requests	✓	✓	✗	✗
Express obligations regarding de-identified data	✓	✓	✗	✗
Requirement to perform data protection impact assessments	✓	✓	✓	✓
Right of private action	✗	✗	✓	✓
Governmental enforcement entities	Attorney General, District Attorneys	Attorney General	CPPA, Attorney General	DPAs
Penalties	Fines governed by Colorado Consumer Protection Act. Up to $20,000 per violation.	Up to $7,500 per violation	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever is higher, in the case of less severe violations. Up to €20 million or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	July 1, 2023	January 1, 2023	January 1, 2023	May 25, 2018

	UTAH CPA	GDPR
Right to opt-out of sale	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-out	Opt-in
Statutory cure period for violations	✓	✗
Right to appeal denials of requests	✗	✗
Express obligations regarding de-identified data	✓	✗
Requirement to perform data protection impact assessments	✗	✓
Right of private action	✗	✓
Governmental enforcement entities	Attorney General	DPAs
Penalties	Fines governed by Utah Consumer Protection Act. Up to $7,500 per violation.	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever is higher, in the case of less severe violations. Up to €20 million or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	December 31, 2023	May 25, 2018

Virginia vs. California vs. Colorado Distinctions

Issue	Colorado (CPA)	Virginia (CDPA)	California (CCPA/CPRA)
Applicability threshold	100k CO records/ data brokers	100k VA records/ >50% of revenue from selling	$25M revenue/50k records/ >50% of revenue from selling (CPRA – 100k records)
Publicly available Information	Broad definition	Broad definition	CCPA – narrow definition CPRA – broad definition
Sensitive Information	Opt-in	Opt-in	Opt-out
Sale	Monetary **or other valuable consideration**	Monetary consideration	Monetary **or other valuable consideration**
Response Time	45 days	45 days	45 days
Cure Period	60 day cure period "if a cure is deemed possible"; expires January 1, 2025	30 day cure period	30 day cure period (CPRA – **NO CURE PERIOD**!)
Private Right of Action	NONE	NONE	Security breaches

Utah Distinctions

Issue	UTAH
Applicability threshold	$25M revenue and 100k UT records or >50% of revenue from selling
Publicly available Information	Broad definition
Sensitive Information	Opt-out
Sale	Monetary consideration
Response Time	45 days
Cure Period	30 day cure period
Private Right of Action	NONE

CDPA vs. CPRA vs. CPA vs. UCPA vs. GDPR – Employee Data

- Virginia's CDPA, Utah's CPA and Colorado's CPA narrowly define "consumer" as "a natural person who is a *[resident of the Commonwealth]/[Colorado/Utah resident]* acting only in an individual or household context".
- The CPRA includes employee data, but extends the employee and business-to-business (B2B) exemption to January 1, 2023, allowing two years for the California Legislature to address employee and B2B privacy questions in a separate bill (two bills on this point).
- Note, however, that all parts of the CCPA that currently apply to B2B and HR contacts continue to apply.

Getting Started – Compliance Project Planning

- Functional Areas – data mapping, contracts, consumer rights
- Personnel – how much can be accomplished by legal versus cross-functional teams
- Timing – Internal completion timelines plus public launch dates
- Budgeting Issues

US DPA Updates Overview

Most negotiated provisions:

- Use rights for technology providers
- Collaboration on notice and consent requirements
- Audit – are summaries of third party audits sufficient
- Breach notice, indemnification and limitation of liability

EU Style DPAs Arriving

New laws in Virginia, Colorado and Utah require companies (if at least one of the parties is subject to at least one of the laws) to sign EU-style agreements establishing the roles of "controller" and "processor"

Internal Risk Analysis

For California, no update may be required if use rights are sufficiently narrow and DPAs already meet GDPR standards

Timing

Now is the time to start updating forms and existing agreements

Strategies for Regulatory Interfacing

- What has been the experience so far?
- How much guidance is available outside of enforcement actions?
- How to effectively explain your organization's overall compliance plan and documentation?

Cookie Banners – Many Considerations

- Notice and Consent under the CCPA (and an enforcement priority)
- New rights under CA, CO, and VA Laws
- Session replay - defense against wiretap claims
- UX Considerations?

Data Brokering – Registration Decisions

State Laws

- A company is a data broker under, generally speaking, if the company sells “the personal information of a consumer with whom [it] does not have a direct relationship.”
- Laws in California, Nevada and Vermont
- Implications for third party data collection.

Broad Applicability

- The broad definition of sale, i.e., under the CCPA, have expanded the scope of such laws
- Thousands of companies have registered as data brokers under the CA law

Other Considerations

- Whether to register as a data broker may shape overall strategy, i.e., whether to sell PI
- Originations must determine whether leadership is comfortable registering, e.g., for reputational reasons

Biometrics Laws – State and Local

- **Consent-Based Laws:** Illinois, Texas and Washington have consent based laws (little enforcement activity in TX & Wash.)

- **Employment laws:** e.g., employers must provide an alternative to fingerprinting in New York

- **Breach laws:** e.g., NY Shield Act and California

- **Regional Divergence:** Certain municipalities, e.g., Portland and NYC, are regulating biometrics at the local level

Artificial Intelligence – State, Local and Federal

- **NYC:** Restrictions on using AI for employment decisions

-**State laws:** Rights to opt out of profiling and automated decision-making

-**FTC:** Enforcement Priority

Looking Ahead

- Additional CA AG Opinions & Enforcement Actions
- Amendments to Existing Laws (VA amended and CPRA amendments proposed)
- New State Laws
- New Privacy Shield
- California & CO AGs to Release Regulations
- Georgia Law – A unique Approach

Any Questions?