BRYAN CAVE LEIGHTON PAISNER BCLP

PREPARING FOR THE NEXT GENERATION OF US DATA PRIVACY LAWS

February 23, 2022

Presenters

Amy de La Lama
Global Chair of Data Privacy and Security
Boulder
amy.delalama@bclplaw.com
+1 303 417 8535

Kim Richardson
Chief Privacy Officer
Verily
kimrichardson@verily.com

Goli Mahdavi
Senior Associate
San Francisco
goli.mahdavi@bclplaw.com
+1 415 675 3448

Overview of Topics

- High-level overview of the California Privacy Rights Act (CPRA), Colorado Privacy Act (CPA), and the Virginia Consumer Data Protection Act (VCDPA)
- Key concepts introduced by these data privacy laws
- How businesses can efficiently update their privacy programs

California Privacy Rights Act

- CPRA is a ballot initiative passed by California voters in the November 2020 election
- Certain aspects of the law took effect on January 1, 2021, but the bulk of the law takes effect on January 1, 2023 (with a 2022 lookback)
- Law generally draws CCPA closer to GDPR
- Regulations to be published for public comment mid-2022
- Raises the threshold for when an entity becomes a "business" by increasing the threshold amount of personal information that must be processed from 50,000 to 100,000, and drops reference to "devices"
- For now, pulls HR and B2B data into scope
- New privacy bureaucracy

Virginia's VCDPA

- Effective date of January 1, 2023
- Applies to businesses that produce products or services that are targeted to Virginia residents and either:
  - Control or process the personal data of 100,000 consumers
  - Control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data
- Does not include personal data that is from an individual in a commercial or employment context (definition of consumer) (HR/B2B carve-outs)

Colorado's CPA

- Effective date of July 1, 2023 (six months after Virginia)
- Applies to businesses that produce products or services that are targeted to Colorado residents and either
  - Control or process the personal data of at least 100,000 consumers (in a calendar year)
  - Control or process the personal data of at least 25,000 consumers and derive revenue or receive a discount on the price of goods or services from the sale of personal data
- Also omits employee and B2B data from the definition of "consumer"
- Notably lacks an exception for nonprofit organizations

What's New?

- Minimization and retention restrictions
- Creation of "sensitive" data category and governing rules
- New data subject rights
- New "Sharing" concept & global privacy control
- Additional privacy disclosures (information disclosures/privacy policies)
- New contracting requirements with service providers/vendors
- Data Privacy Impact Assessments
- Expansion of private right of action to username and password breach

Minimization & Retention Restrictions

- New requirement for businesses to minimize the data they process and not store data for longer than is reasonably necessary
- Very similar to GDPR concept and effectively requires businesses to create a ***data map***
- **Action Item(s):**
  - Complete data mapping exercise
    - For CA, be sure to consider B2B and employee data
  - Update data retention policy and retention schedules and develop strategy for implementing company-wide

Sensitive Data and Governing Rules

- New broad category of sensitive data added - similar to GDPR but also including data we see in breach notification laws and other unique data such as precise geolocation.

- **Action Item(s):**
  - Identify sensitive data and determine if an exemption applies (e.g. HIPAA, GLBA, etc.)
  - Provide specific disclosures around use of sensitive data
  - Implement mechanisms for people to exercise right to limit use (CPRA)
  - Obtain consent when required (CPA and VCDPA)

New Data Subject Rights

- In addition to the CCPA rights, CPRA/CPA/VDCPA provide consumers with new rights, including:
  - Right to correction
  - Right to opt-out of Automated Decision Making (including profiling) and right to access information regarding the same
  - Right to restrict processing of Sensitive Personal Information (CPRA), or opt-in to the use (CPA and VCDPA)
- **Action Item(s):**
  - Develop or update existing consumer rights ("Data Subject Rights") response procedures and templates

Targeted Advertising & the Introduction of New "Sharing" Concept

- CPRA's definition of sharing takes direct aim at cookies and other cross-contextual advertising
- CPA/VDCPA: opt-out right for "targeted advertising"
- Global Privacy Control
- **Action Item(s):**
  - Evaluate current cookie consent strategy, with particular emphasis on understanding what cookies and similar technologies are utilized by your business and what may be a "sale" or a "sharing"
  - Implement opt-in consent (subject to additional guidance) or "Do Not Sell/Share My Personal Information" link as appropriate

Information Notices (Privacy Policies)

- New features of the laws also require enhanced privacy notices
- **Action Item(s):**
  - Update Privacy Notice to include additional disclosures around (i) the new and expanded data subject rights, (ii) sensitive personal information collection practices, (iii) data retention, and (iv) information "sharing" practices
  - Evaluate/update current privacy notice update and distribution strategy for employees, job applicants and other third party B2B contacts currently subject to exceptions under the CCPA

Vendor Management

- New set of vendor flowdown requirements that will require covered businesses to revisit data processing agreements with service providers/vendors
- **Action Item(s):**
  - Evaluate existing data protection terms in place with vendors and develop action plan with regard to updating those terms at a pace and sequence that is workable (e.g., at time of renewal or prioritizing by importance) and amend as needed

Data Processing Impact Assessments

- Mandatory Risk Assessment for high risk processing (like GDPR's DPIA concept)
- Must be made available to the regulator
- **Action Item(s):**
  - Identify any activities that present a high risk to personal data protection and privacy
  - Develop template(s) for internal record-keeping concerning the impact of high risk processing

Expansion of Private Right of Action (CPRA)

- The CPRA adds a new category of data for which a private cause of action may be brought: "email address in combination with a password or security question and answer that would permit access to the account"
- Clarifies that maintaining reasonable security procedures does not amount to a "cure"
- **Action Item(s):**
  - Benchmark documentation of existing WISP against industry best practice
  - Review existing incident response plan for compliance with the CPRA/CPA/VDCPA and best practices
  - Revise or rewrite the incident response plan (as needed) to close any identified gaps

Key Takeaways

- Engage in strategic decision making
- Engage key stakeholders early
- Perform data mapping exercise to inform scope of compliance obligations
- Evaluate exemptions that may apply to your business or a particular data set
- Update disclosures and contracts
- Develop strategies for managing consent and limitations for cookies and sensitive data

BRYAN CAVE LEIGHTON PAISNER BCLP

bclplaw.com

[This document] provides a general summary and is for information/educational purposes only. It is not intended to be comprehensive, nor does it constitute legal advice. Specific legal advice should always be sought before taking or refraining from taking any action.

604694989.2