Data Privacy and Security Updates for 2022 and Beyond: What Employers Need to Know

Michael Gentry
Shareholder
Office: 414-298-8715
mgentry@reinhartlaw.com

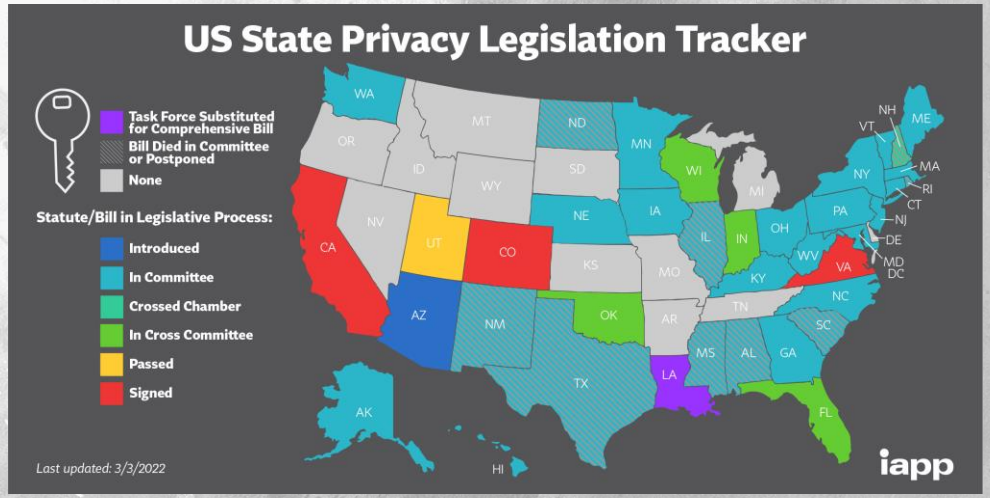
Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Data Privacy and Security Update

- Evolving State Patchwork of Comprehensive Data Privacy Laws
- Federal action update
  - FTC and DOJ activity
  - Recent legislation
- Updating Handbooks and Agreements for Data Security

Evolving Patchwork of State Laws

- California Consumer Privacy Act (CCPA): 2020
- Virginia Consumer Data Protection Act: 2023
- Colorado Privacy Act: July 2023
- Utah Consumer Privacy Act: 2024?
- Wisconsin: 2024?



https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Evolving Patchwork of State Laws

- What's specific to a comprehensive data privacy law?
  - Notice to consumers/ data subjects
  - Right of Access
  - Right of Rectification
  - Right of Deletion
  - Right of Restriction
  - Right of Portability
  - Right to Opt-Out
  - Other rights

Evolving Patchwork of State Laws

- Determining whether state data privacy laws apply
- https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/

	CCPA	CPRA	VCDPA	CPA
Jurisdictional threshold	"Does business" in California	"Does business" in California	"Conduct business" in Virginia or produce products or services "targeted" to Virginia residents	"Conducts business" in Colorado or produces or delivers commercial products or services "intentionally targeted" to Colorado residents
Revenue threshold	Annual gross revenues greater than $25 million	Annual gross revenues greater than $25 million in preceding calendar year	None	None
Processing threshold	Data of 50,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers	Data of 100,000 or more consumers
Broker threshold	At least 50% of revenue from selling of data	At least 50% of revenue from selling or sharing of data	Data of 25,000 or more consumers + at least 50% of revenue from sale of data	Data of 25,000 or more consumers + derives revenue or receives discount from sale of data

Evolving State Patchwork of Applicable Laws

- Wisconsin Assembly Bill 957, which would create Wis. Stat. Sec. 134.985, regulating data protection for Wisconsin consumers
  - Wisconsin State Assembly voted 59-37 to pass on February 23, 2022
  - Senate adjourned on March 10 without taking up the bill
  - Will need to be reintroduced next session
  - Modeled after Virginia's law; generally,
    - Notice to consumer of what is collected and for what reason; delete; port; opt-out of targeted advertising

Evolving Patchwork of Applicable State Laws

- California Privacy Rights Act, effective January 2023
  - Privacy law now applies to employment data
  - Changes the thresholds for “businesses” under the CCPA
  - Established the California Privacy Protection Agency
  - The right to correct inaccurate personal information
  - The right to limit the use of "sensitive personal information”
  - The right of no retaliation

Federal Action: Recent Legislation

- President Biden's State of the Union Address
- Strengthening American Cybersecurity Act
- Banning Surveillance Advertising Act
- Promoting Digital Privacy Technologies Act
- U.S. House Committee on House Administration hearing: "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors."
- No preemptive legislation

Federal Action: Federal Trade Commission

- FTC Safeguards Rule expanded in October 2021
  - Applies to more organizations
  - Strengthened the data security safeguards that financial institutions are required to put in place to protect their customers' financial information
  - Limit who can access consumer data and use encryption to secure the data
  - Explain their information sharing practices
  - Designate a single information security professional

Federal Action: Department of Justice

- On October 6, 2021, DOJ launched new Civil Cyber-Fraud Initiative.
- Seeks to "utilize the False Claims Act ("FCA") to pursue cybersecurity related fraud by government contractors and grant recipients."
- DOJ will seek FCA penalties from government contractors or grant recipients that knowingly falter on their cybersecurity responsibilities.
- Potential for treble damages and per-claim monetary penalties for violating cybersecurity representations.
- Qui Tam actions by whistleblowers

Updating Handbooks and Agreements

- Comprehensive Data Security Policy/Program
- Employee Handbook Updates
  - Remote Work Policy/Program
  - Employer Technology Policy/ Terms and Agreements
  - Confidentiality Policy
  - BYOD device policy
  - Electronic Communications Policy
  - State by State Supplements or Revisions due to Remote Employees

Updating Handbooks and Agreements

- Develop and/or Update Agreements with Employees
  - Employment Agreements
  - Confidentiality

- Review agreements with vendors and independent contractors
  - CPRA will require new language and notice for any California-based independent contractor agreements
  - Vendor relationships involving data based in Colorado, Virginia and California