



PROGRAM MATERIALS
Program #30200
September 17, 2020

**In the Cannabis Industry, Profitability
and Data Privacy/Security go
Hand-in-Hand**

**Copyright ©2020 by Rebecca Rakoski, Esq. - XPAN Law
Group
All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

In the Cannabis Industry, Cybersecurity/Data Privacy and Profitability Go Hand-In Hand

Rebecca L. Rakoski, Esquire
XPAN Law Group, LLC



The Cannabis Industry

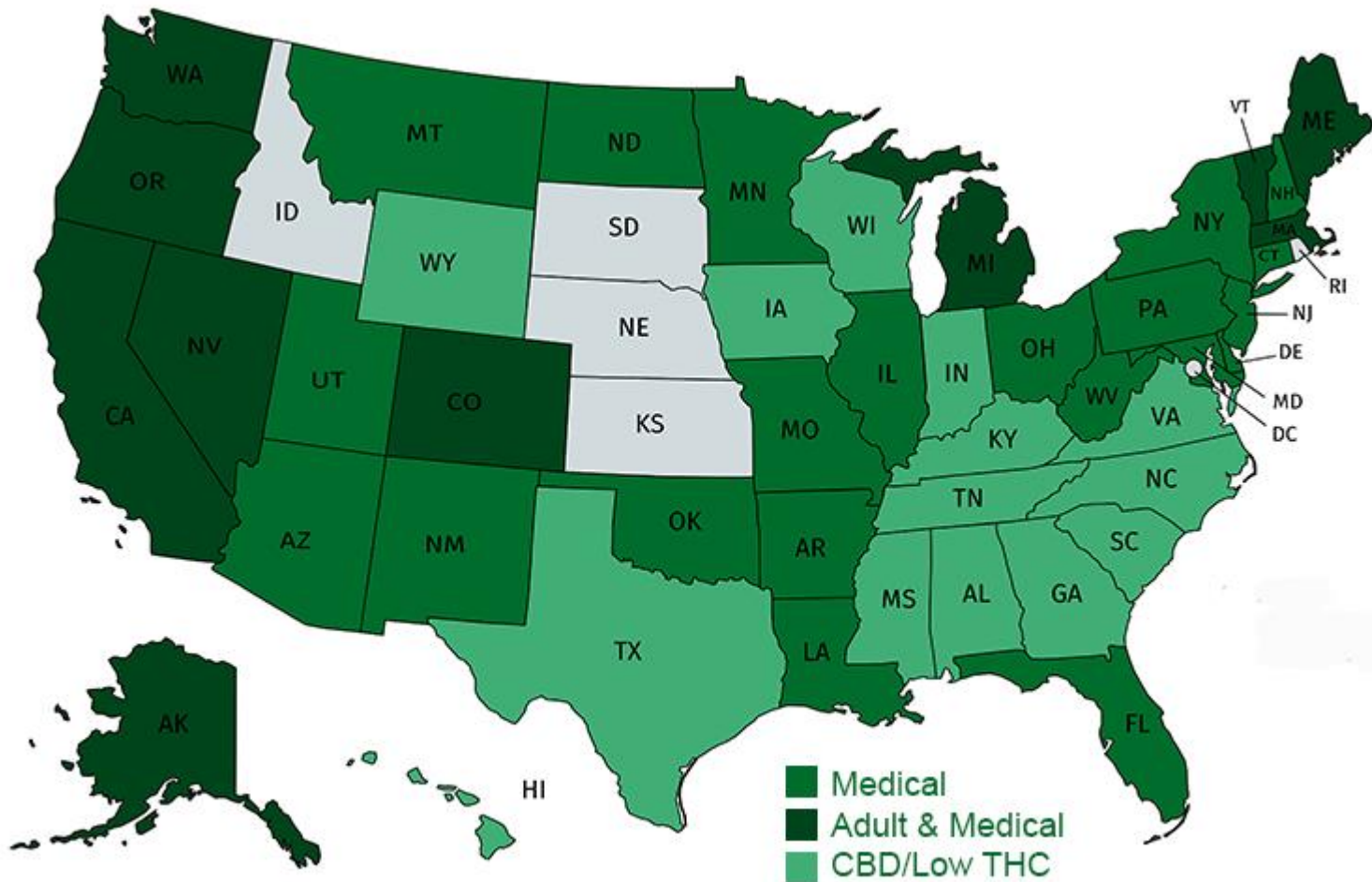
- Legalized cannabis industry is growing domestically and moving into the highly profitable European Marketplace
- Cannabis is already legal in Colombia and Portugal
- Hemp, source for CBD, will expand *internationally* to \$2.1 billion in consumer sales by the end of 2020



The Cannabis Industry, Cont'd

- Real Medical Testing is Increasing
- Customers will Expand Purchases Beyond Medical Uses (i.e. recreational use particularly in older consumers)
- Legislative Actions Will Be Robust
- Profitability Remains Elusive





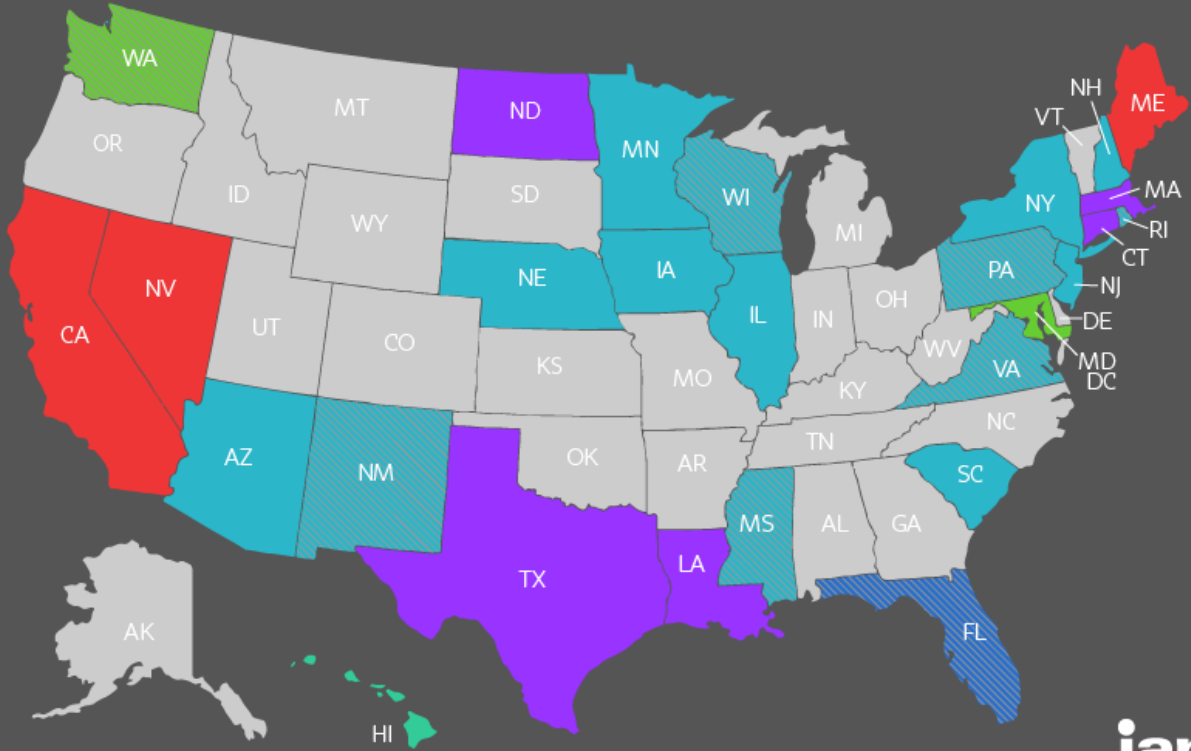
State Comprehensive-Privacy Law Comparison



- Task Force Substituted for Comprehensive Bill
- Bill Died in Committee or Postponed
- None

Statute/Bill in Legislative Process:

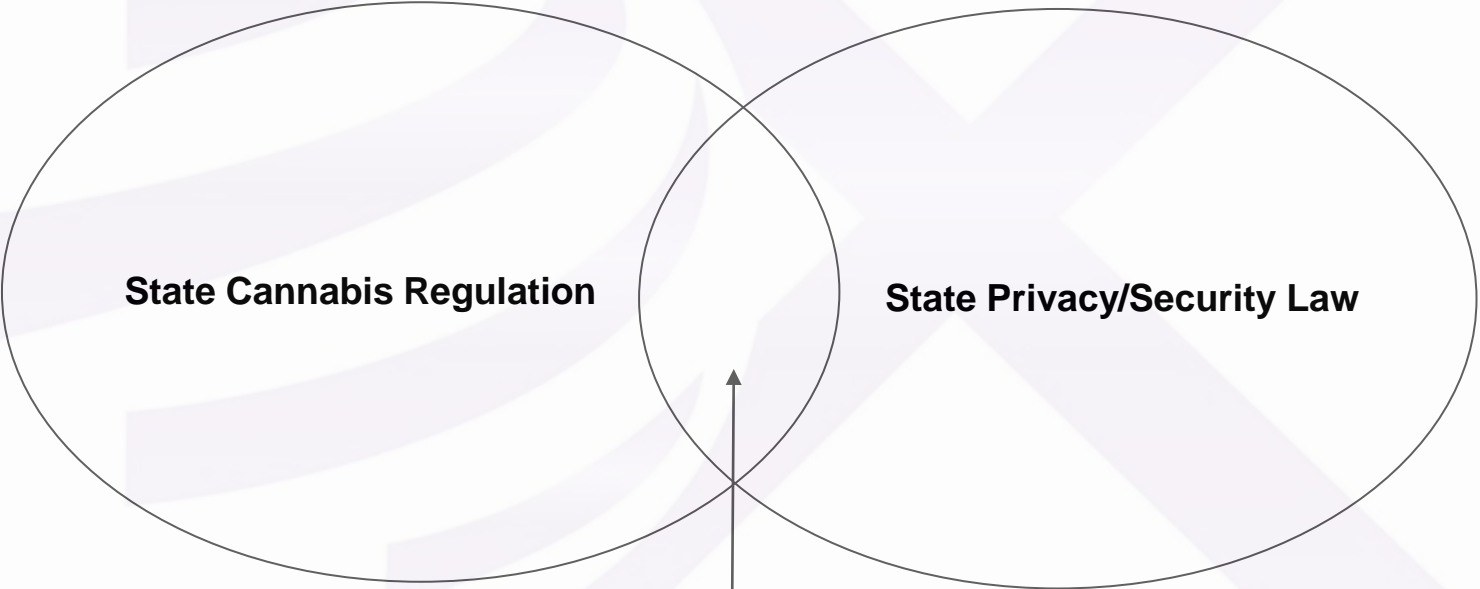
- Introduced
- In Committee
- Cross Chamber
- Cross Committee
- Passed
- Signed



Last updated: 7/6/2020

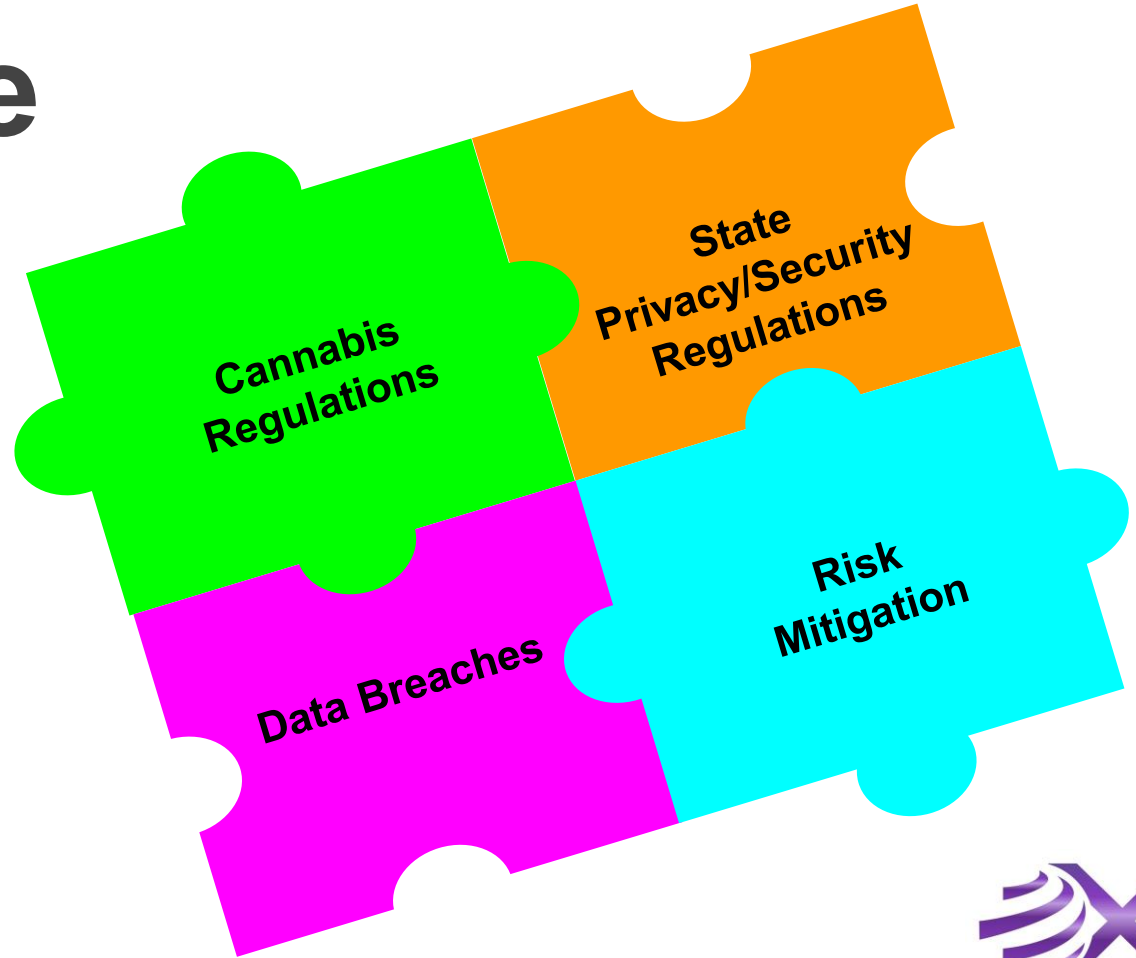


INTERSECTION



LIABILITY

The Puzzle



Data leak strikes 115 cannabis users, sensitive information exposed



A database backing point-of-sale systems used in n

na dispensaries has been compromised.

Report: Cannabis Users' Sensitive Data Exposed in Data Breach

Case in Point: California Cannabis Regulations

- California Cannabis Track-and-Trace



- METRC (Marijuana Enforcement Tracking Reporting Compliance)



Consumer Data

- First and Last Name
- Address
- Copies of Driver's Licenses or Identification Cards
- Social Security Number
- Health-related data



California Consumer Privacy Act of 2018 ("CCPA")



Overview of the CCPA

The CCPA applies to the collection of private information related to a “consumer.” Cal. Civ. Code § 1798.140(g).

Consumer:

- A “natural person who is a California resident.” Cal. Civ. Code § 1798.140(g).
- Includes:
 - “every individual who is in California for other than a temporary or transitory purpose,” and
 - “every individual domiciled in California who is outside the state for a temporary or transitory purpose.” Cal. Code Regs. tit. 18, § 17014.



Overview of the CCPA

To trigger the requirements of the CCPA, a business must qualify as any legal entity that operates for profit in California and:

- Has gross revenues exceeding twenty-five (25) million dollars;
- Buys, receives, sells, or shares personal information of more than 50,000 consumers, households, or devices; *or*
- “[D]erives 50 percent or more of its annual revenues from



Overview of the CCPA

The CCPA applies to the collection of personal information related to a “consumer.” Cal. Civ. Code § 1798.140(g).

Personal Information

- “[I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly, or indirectly, with a particular consumer or household.” Cal. Civ. Code § 1798.140(o)(1).
- Includes (Cal. Civ. Code § 1798.140 (o)(1)(A)):
 - biometric information,
 - internet network activity,
 - geolocation data,
 - education information, and
 - passport numbers.



Limitations on Rights Under the CCPA

- **Certain Rights**

- **Right to request** certain information;
- **Right to opt-out** of the sale of personal information about the consumer; and
- **Right to deletion** of any personal information.

- **Twelve (12) Month Limitation:**

- Applies to Rights to request and right to opt-out
- Limits the information provided to the preceding 12 months of data collection

- **Right to deletion** has nine (9) exemptions



Website & Notice Requirements

Must be provided at or before the point of collection of information and include the following:

- The categories of information the business collects and the purposes;
- Consumers' data rights;and
- If the business intends to sell personal information to third parties, the right of the consumer to opt out from that sale.

Website Privacy Notice:

- Review & Update Privacy Notice at least once every 12 months.
- A clear and conspicuous link titled **“Do Not Sell My Personal Information,”** to a webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information.



Service Provider Requirements

Regulates how businesses share consumer information with third parties and service providers.

- “Service provider”:
 - A legal entity organized for profit or the financial benefit of shareholders with which a business discloses personal information of consumers for a business purpose. Cal. Civ. Code § 1798.140(v).
- “Third-Parties”:
 - Entities that are not businesses or service providers are considered third parties under the CCPA. Cal. Civ. Code § 1798.140(w).



California Privacy Rights Act (“CPRA”)

- Qualified for the November 2020 ballot initiative
- Key Provisions:
 - Establish the California Privacy Protection Agency (“CPPA”)
 - Defines “sensitive personal information” stricter than personal information
 - Creates new obligations for companies and organizations processing sensitive personal information. It would also allow consumers to limit the use and disclosure of their sensitive personal information.
 - Additional Consumer Rights
 - Expanded Moratorium for Employee Data until January 1, 2023
 - Expanded Breach Liability



Health-Related Data



The Challenge: International

Cannabis, Cybersecurity and Data Privacy

September, 2020



EU General Data Protection Regulation

Applies to the “processing” and free movement of “personal data” of “natural persons” within the EU

- Are you impacted by the GDPR?
- If you are impacted, what is your role?
 - ◆ **Controller, Joint Controller, Processor, Sub-processor**
- How do you comply?
 - ◆ Documentation
 - ◆ Processes



The Solution

Cannabis, Cybersecurity and Data Privacy

September, 2020



COMPLIANCE

THE LAW

TECHNOLOGY

**RISK
MITIGATION**

1. Understand What Regulations Impact You

2. Cross-Map Your Requirements

3. Understand Your Contractual Obligations

4. Identify Your Network Vulnerabilities

5. Document in written policies & procedures

6. Training & Communication



Key Trends in 2020 to Keep in Mind

**Pending &
New Laws**

**Brexit &
the Cross-
Border
Flow of
Data**

**Growing
Court &
Agency
Enforcement**

**Individuals
enforcing
their rights**



Key Takeaways

- Address weak, or underdeveloped, data security and data privacy practices.
- Use knowledgeable counsel that understands the industry AND the data privacy/security issues surrounding the data.
- Vet third party vendors.
- Examine insurance coverage annually.
- Create processes and procedures to establish (i.e. prove) compliance.





***For further information or questions, please contact me at:
rrakoski@xpanlawgroup.com***

Disclaimer: These materials do not constitute legal advice. The speakers do not warrant that the presentations or materials are free of errors, or will continue to be accurate. Opinions expressed are those of the speakers and statements in the presentations and the materials should be verified before relying on them.

