How Cannabis Cos. Can Keep Up With Privacy Compliance

By **Brett Schuman, Jacqueline Klosek and Joshua Fattal** (March 16, 2023)

Brett Schuman

Jacqueline Klosek

Joshua Fattal

The size of the cannabis industry has skyrocketed since the first states, Colorado and Washington, legalized cannabis for adult recreational use 10 years ago.

The latest statistics indicate that the industry has grown over 400% to $25 billion, with projections estimating the market to be worth $55 billion by 2026.[1]

As of this date, 21 states and Washington, D.C., have legalized cannabis for adult use. Thirty-seven states and Washington, D.C., have legalized cannabis for medical use, and 31 states and Washington, D.C., have decriminalized cannabis, removing criminal penalties for activities such as low-level possession.[2]

With the rapid growth of the cannabis industry, the ever-changing patchwork of U.S. state-by-state data privacy and cybersecurity laws and the fact that companies operating in the cannabis industry often have access to sensitive information, it is becoming increasingly important for cannabis companies to treat privacy and cybersecurity as a significant risk and management priority.

Several recent highly publicized data breaches in this space, discussed in more detail below, have only underscored the urgency surrounding these issues.

Keeping Up Compliance with State Privacy Laws

Since its implementation in 1970, the Controlled Substances Act treats cannabis as a Schedule I drug.[3]

A person violates federal law for mere possession — in addition to trafficking and other offenses — under the CSA.

Although President Joe Biden recently pardoned all federal possession offenses through executive order and urged governors to do the same,[4] mere possession of cannabis remains a federal crime punishable at least in theory by imprisonment and a fine.

Many states have therefore taken matters into their own hands, legalizing cannabis for adult recreational use or medical use. California first legalized medical cannabis in 1996.

While at the federal level, there are many privacy laws that govern specific, sector-based issues, with respect to general, broad-based consumer data laws, it is the states that are key.

Although Congress introduced the American Data Privacy and Protection Act[5] in the summer of 2022, the bill has stalled in committee, and states have continued to step in to fill the gap.

Two states, California and Virginia, have comprehensive data privacy laws that are currently in effect. Similar legislation in Colorado, Connecticut and Utah is taking effect later this year.[6] All of these states, except Utah, have legalized cannabis for recreational use.

While each state's privacy law differs slightly from the others, they all require companies to post a privacy policy notifying consumers of the rights they have in relation to their personal information, and they all require companies to offer consumers the right to access, correct and delete their data.

For certain consumers of cannabis products, who may be hesitant to publicize their usage of the substance and eager to remove records of their purchases, the right to delete may be particularly appealing, though it comes with important limitations that cannabis companies need to understand and be able to implement.

The legalization of recreational and medical cannabis has allowed dispensaries in many states to collect troves of information about their consumers, whether mandated by law or regulation or by personal choice, often without being subject to particular requirements for the protection of consumers' data.

Some states' legalization laws, like Maine's Cannabis Legalization Act,[7] make no mention of data privacy at all, allowing dispensaries to collect as much information as they want.

Colorado does not prohibit the collection of any personal information, but it does not require dispensaries "to acquire and store personal information."[8] Effectively, these states permit dispensaries to collect as much consumer personal information as they choose to.

Still, other states have taken a different approach. Illinois' cannabis law is more stringent with respect to data privacy, requiring consumers to provide opt-in consent before a dispensary collects personal information.[9]

Other states, such as California, have amended their cannabis laws to regulate data privacy. Under the Medicinal and Adult Use Cannabis Regulation and Safety Act, dispensaries in California cannot disclose certain categories of a consumer's personal information to a third party except to the extent needed to process the transactions, i.e., payment information.[10]

Oregon has gone as far as to prohibit dispensaries from recording or retaining any information that may be used to identify a consumer.[11]

While state cannabis regulations provide some protection in certain states, the states that have passed comprehensive data privacy laws are now providing additional protections to consumers and placing more requirements on businesses.

For example, the Medicinal and Adult Use Cannabis Regulation and Safety Act's definition of personal information is very narrowly tailored — it only includes a person's first and last name in combination with another identifier such as a driver's license.

However, California's comprehensive privacy law, the California Consumer Privacy Act, as recently amended by the California Privacy Rights Act, imposes requirements on businesses that maintain any data that can reasonably identify a person.[12]

In states such as California, dispensaries need to comply with both the state's cannabis regulation as well as the state's comprehensive privacy regulation — where applicable —

and need to account for the fact that one law may contain broader rights than the other.

While dispensaries offering recreational cannabis typically collect personal information such as name, date of birth and address — information appearing on a typical driver's license — dispensaries offering medical cannabis collect even more sensitive data about their customers.

In some states, in order to obtain a medical cannabis card, a patient must first be diagnosed by a doctor with one of the qualifying ailments listed in the state's medical cannabis statute.

Once diagnosed, the patient must then present an ID and their medical cannabis card at a medical dispensary. Just going to a medical dispensary alone may implicate a consumer's sensitive health information.

While many dispensaries have assumed that the Health Insurance Portability and Accountability Act does not apply to them because cannabis is illegal at the federal level, some commentators are now saying that medical dispensaries may in fact be subject to HIPAA.[13]

However, whether medical dispensaries engage in covered transactions — which would qualify them as covered entities under HIPAA — remains up for debate because dispensaries are not billing health insurance companies for medical cannabis products.

To fill a gap in protection for medical information shared with dispensaries, some state regulators have gone so far as to incorporate HIPAA into the state's cannabis regulations, requiring medical dispensaries to comply with the much broader set of HIPAA compliance obligations.

For example, Illinois requires dispensaries to comply with HIPAA through the Compassionate Use of Medical Cannabis Program Act.[14]

Taking Cybersecurity Seriously

Given the vast amount and the sensitivity of data that dispensaries are collecting, cannabis companies have become a frequent target of cyberattacks.

Many newer dispensaries, and even established ones, which have not yet implemented industry-standard cybersecurity protections, are facing attacks. In 2019, for example, 30,000 customers were affected by a data breach that exposed the patients' full names, dates of birth, and the price and quantity of cannabis purchased over time.[15]

In another breach in 2020, a dispensary was subject to a phishing attack, where the threat actor stole and then offered to sell personal information of cannabis customers, including images of passports, checks and driver's licenses, on a hacker forum in exchange for bitcoins.[16]

As dispensaries have matured, they have begun to utilize cloud-based point-of-sale systems and data science software to gain insight into their customer base. While more can be done to protect consumer information in these systems, cloud-based systems are typically more secure than data storage on-premises.

Dispensaries adopting these measures may be improving their company's data security,

sometimes even without knowing it.

But given the current state-by-state patchwork of data breach notification laws, most of which explicitly require notification in the event of unauthorized access to driver's licenses — the very information that many dispensaries collect — dispensaries should consider doing more to prioritize information security before it is too late.

Compliance Recommendations

Companies in this space should take seriously their privacy and cybersecurity obligations not only to comply with applicable legal requirements, but also to set their businesses up for success in the next financing round or investment.

We anticipate seeing continued investing, lending and acquisitions activity in the years ahead as more states legalize cannabis for medical or recreational use, and privacy and cybersecurity compliance continues to be an increasingly central focus of the legal due diligence process.

To better prepare themselves for the compliance challenges and diligence processes ahead, we recommend that cannabis companies take the following steps.

Companies should prepare an externally facing privacy policy that describes the company's data collection and handling practices and establishes the applicable rights of consumers, and make this notice available to consumers at all data collection points, such as websites and mobile apps.

Companies should conduct periodic reviews of externally facing privacy policies to ensure compliance with new privacy laws and amendments to existing laws.

Businesses should also honor consumers' data subject requests, such as the right to delete personal data where required under applicable law and where the commitment to data subject rights has otherwise been made in the company's privacy policy.

Businesses should determine the impact of emerging privacy laws and regulations on the company and consider submitting to compliance audits.

Current state consumer data privacy laws have fairly high thresholds of applicability, so smaller companies are not likely to be regulated directly as larger businesses or controllers under such laws.

However, they may be affected if they are providing services for other companies who are covered by these laws. Moreover, this is a rapidly evolving area of law, with more states proposing their own versions of these laws, so it should be monitored closely.

Companies should subject to the overarching requirement to comply with local law and regulations, minimize the amount of sensitive consumer data the company collects, and only store data for as long as necessary to achieve the business purpose of data collection.

Companies should implement security measures to protect consumer data, including maintaining a comprehensive, written information security program that includes administrative, technical and physical safeguards designed to protect consumer data.

Businesses should conduct system-wide penetration testing and vulnerability assessments

at least annually, and promptly remediate any areas of concern, with an immediate focus on vulnerabilities classified as having critical or high-level importance.

Companies should also develop an incident response plan to be prepared in the event of a data security incident. They should also train employees on privacy requirements and cybersecurity best practices.

Lastly, businesses should develop, implement and maintain a comprehensive vendor management program that includes conducting diligence on third-party service providers' data protection measures and implementing appropriate agreements with all service providers.

Brett Schuman is a partner and co-chair of the IP litigation business unit at Goodwin Procter LLP.

Jacqueline Klosek is a partner at the firm.

Joshua Fattal is an associate at the firm.

Goodwin associate Madeline Fuller contributed to this article.

[1] Available at https://www.forbes.com/sites/andrewdeangelo/2022/10/04/the-hockey-stick-turns-into-bell-curve-a-new-report-from-bdsa-sheds-light-on-cannabis-industry-growth/?sh=20ef3e0666f2.

[2] Includes states listed by the Marijuana Policy Project as having an effective medical cannabis program. For more information, see https://www.mpp.org/states/.

[3] 21 U.S.C. § 812; 21 C.F.R. § 1308.11.

[4] Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/06/granting-pardon-for-the-offense-of-simple-possession-of-marijuana/.

[5] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[6] For a summary of enacted and pending state privacy laws, see https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison.

[7] Me. Rev. Stat. tit. 28-B, § 511.

[8] Colo. Rev. Stat. Ann. Colo. Const. Art. XVIII, § 16 (Use and Regulation of Marijuana) (West 2018).

[9] 410 Ill. Comp. Stat. Ann. 705/1 (West 2019).

[10] Cal. Bus. & Prof. Code §§ 26150-26156 (2016).

[11] 17 Or. Rev. Stat. Ann. § 475B.220 (West 2017).

[12] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (West 2018), as amended California Privacy Rights Act.

[13] For further discussion, see https://www.jdsupra.com/legalnews/are-medical-marijuana-businesses-61349/.

[14] 410 Ill. Comp. Stat. Ann. 130/1 (West 2023).

[15] Available at https://www.zdnet.com/article/data-leak-strikes-us-cannabis-users-sensitive-information-exposed/.

[16] Available at https://www.bleepingcomputer.com/news/security/hacker-sells-aurora-cannabis-files-stolen-in-christmas-cyberattack/.