2021

Comment: Dude Where's My Data: The Intersection of Data Privacy Law and the Marijuana Industry in the United States

Andrew B. Broome

Andrew Broome

Comment Final Draft

Advisor: Professor Opderbeck

4/10/2020

Comment: Dude Where's My Data: The Intersection of Data Privacy Law and the Marijuana Industry in the United States

A growing concern amongst consumers who purchase marijuana is how their personal data is being collected, and, more specifically, how that data is being used. A tension exists between protecting the privacy of consumers who are concerned about the stigma associated with purchasing marijuana and the desire to restrict interference in commercial activities. This paper serves to explore what legislative measures states, where marijuana has been legalized recreationally, have done to ensure the protection of consumer data, and if a model exists for other states seeking to legalize marijuana recreationally to follow suit. Part I of this paper will provide an introduction to the marijuana industry in the United states, as well as its illegal classification at the federal level. Part II will provide an overview of data privacy law in the United States and discuss the tension between the value of data in commercial activities and the right for consumers to have their personal data protected. Lastly, Part III will analyze data privacy law in the United States, at the state and federal level, in the context of the legal marijuana industry, and provide potential solutions to current issues.

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[1]

I. Introduction

A. The Marijuana Industry in the United States

The legal marijuana industry is one of the fastest growing industries in the United States.[2] In 2018, the industry grew to over $10.4 billion, and provided jobs to over 250,000 people.[3] By

[1] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).
[2] Don Reising, *The Legal Marijuana Industry Is Soaring—And 2019 Could Be Its Best Year Yet*, FORTUNE (Dec. 27, 2018), https://fortune.com/2018/12/27/legal-marijuana-industry-sales/
[3] *Id.*

the end of 2019, medical and recreational marijuana sales in the United States are on pace to surpass $12 billion.[4] In California alone, annual sales of marijuana are forecasted to exceed $5.6 billion in 2020, and over $6.5 billion in 2025.[5]

Currently, 33 states have legalized marijuana for medicinal use.[6] Regarding its medicinal purposes, the Food and Drug Administration ("FDA") has approved the use of marijuana for treatment of Dravet Syndrome and Lennox-Gastaut Syndrome—two rare forms of epilepsy, but doctors routinely prescribe it for various other ailments, e.g., Alzheimer's disease, Cancer, Mental health conditions, and Chrohn's disease.[7] As of 2019, 11 states and Washington, DC have authorized the recreational use of marijuana for individuals over the age of 21.[8] The trend for state recreational legalization is growing, with approximately 62% of Americans in favor its legalization.[9] However, there are risks associated with the marijuana industry because it remains illegal at the federal level;[10] for example, business owners with marijuana assets and securities are in jeopardy of civil or criminal forfeiture.[11]

Albeit states are relaxing their approach towards the recreational and medicinal use of marijuana, at the federal level marijuana is still classified as a Schedule 1 drug under the

---

[4] Eli McVey, *Exclusive: US Retail Marijuana Sales on Pace to Rise 35% in 2019 and Near $30 Billion by 2023*, MARIJUANA BUSINESS DAILY (May 30, 2019), https://mjbizdaily.com/exclusive-us-retail-marijuana-sales-on-pace-to-rise-35-in-2019-and-near-30-billion-by-2023/

[5] https://blog.rsisecurity.com/is-your-data-safe-when-you-purchase-at-a-legal-weed-dispensary/

[6] Jeremy Berke & Skye Gould, *Illinois Just Became the First State to Legalize Marijuana Sales Through the Legislature—Here Are All the States Where Marijuana is Legal*, BUSINESS INSIDER (Jun. 25, 2019, 1:52 PM) ("If your Canadian marijuana-buying data ends up on a server in the United States, could it make its way to U.S. border officials? There's little to stop it, privacy experts say.") https://www.businessinsider.com/legal-marijuana-states-2018-1

[7] *Medical Marijuana FAQ*, WEBMD.COM, https://www.webmd.com/a-to-z-guides/medical-marijuana-faq

[8] *Id.*

[9] Hannah Hartig & A.W. Geiger, *About Six-In-Ten Americans Support Marijuana Legalization*, PEW RESEARCH CENTER (October 8, 2018), https://www.pewresearch.org/fact-tank/2018/10/08/americans-support-marijuana-legalization/

[10] Controlled Substances Act, 21 U.S.C.S. § 812.

[11] Sean M. O'Conner & Jason Liu, *The Risks of Clouded Property Title for Cannabis Business Owners, Investors, and Creditors*, 3 TEX, A&M J. PROP. L. 67, 87 (2016).

Controlled Substances Act ("CSA").[12] Congress views Schedule I drugs as the most dangerous kind.[13] Marijuana sits alongside Heroin, LSD, and Ecstasy in the Schedule I class.[14] The states' approach to marijuana legislation does not affect its federal classification according to Supreme Court precedent.[15] In the seminal case *Gonazales v. Raich*, the Supreme Court upheld the federal government's constitutional authority to regulate local activities that are a part of a class of activities having a substantial effect on interstate commerce under the Commerce Clause.[16] Furthermore, Courts have ruled the classification of marijuana as a Schedule I drug is not irrational nor arbitrary.[17]

Although marijuana is illegal under the CSA, the CSA provides state Attorney Generals with discretion in regulating marijuana-related activities at the state level.[18] The CSA states that "[t]he Attorney General may promulgate and enforce any rules, regulations, and procedures which he may deem necessary and appropriate for the efficient execution of his functions under this title."[19] This sort of discretion is largely contingent on the current presidential administration's approach to marijuana enforcement. Since 2009, Attorney Generals Ogden,[20]

[12] Controlled Substances Act, 21 U.S.C.S. § 812(c). The findings required for a drug to be listed as Schedule I are: (a) the drug or other substance has a potential for abuse; (b) the drug or other substance has no currently accepted medical use in treatment in the United States; and (c) there is a lack of accepted safety for use of the drug or other substance under medical supervision.
[13] *Id.*
[14] *Id.*
[15] *See* Gonzales v. Raich, 545 U.S. 1 (2005).
[16] *Id.* at 22 ("[c]oncluding that Congress had a rational basis for believing that failure to regulate the intrastate manufacture and possession of marijuana would leave a gaping hole in the CSA.")
[17] *See, e.g.*, United States v. Greene, 892 F.2d 453, 456 (6th Cir. 1989) (concluding the mechanism used to classify marijuana is rational and marijuana's Schedule 1 classification does not violate due process).
[18] Controlled Substances Act, 21 U.S.C.S. § 871(b).
[19] *Id.*
[20] Memorandum from David W. Ogden, Deputy Att'y Gen., to U.S. Attorneys, Investigations and Prosecutions in States Authorizing the Medical Use of Marijuana (Oct. 19, 2009) [hereinafter Ogden Memo].

Cole,[21] and Sessions[22] have each issued memorandum providing guidance on prosecution in jurisdictions where marijuana is legal. However, Deputy Attorney General Ogden's guidance was restricted to federal prosecutions in states where marijuana is legal for medicinal purposes, not recreational.[23]

In 2011, when medical marijuana dispensaries started to grow larger in scale, Deputy Attorney Cole provided clarification to the interpretation of the Ogden Memo, stating that "[t]he Ogden Memorandum was never intended to shield such activities from federal enforcement action and prosecution, even where those activities purport to comply with state law."[24] When clear trends emerged that states were willing to legalize marijuana not only for medical use, but for recreational use as well, Deputy Attorney Cole issued an additional memo explaining that the federal government will largely defer to states for enforcing marijuana legislation within their borders.[25] And in 2014, Cole issued a memo providing guidance to financial institutions dealing with marijuana-related entities.[26] However, Cole's memo was met with some skepticism amongst federal judges. United States District Judge Richard Jackson stated the following about the guidance document: "In short, these guidance documents simply suggest that prosecutors and

[21]Memorandum from James M. Cole, Deputy Att'y Gen., to U.S. Attorneys, Guidance Regarding the Ogden Memo in Jurisdictions Seeking to Authorize Marijuana for Medical Use (June 29, 2011) [hereinafter Cole Memo I]; Memorandum from James M. Cole, Deputy Att'y Gen., to U.S. Attorneys, Guidance Regarding Marijuana Enforcement (Aug. 29, 2013) [hereinafter Cole Memo II]; Memorandum from James M. Cole, Deputy Att'y Gen., to U.S. Attorneys, Guidance Regarding Marijuana Related Financial Crimes (Feb. 14, 2014) [hereinafter Cole Memo III]

[22] Memorandum from Jefferson B. Sessions III, Att'y Gen., to U.S. Attorneys, Marijuana Enforcement, (Jan. 4, 2018) [hereinafter Sessions Memo].

[23] Cole Memo I, supra note 21.

[24] *Id.*

[25] Cole Memo II, supra note 21.

[26] Cole Memo III, supra note 21.

bank regulators might "look the other way" if financial institutions don't mind violating the law. A federal court cannot look the other way."[27]

The most recent administration took an opposite stance to Attorney Generals Ogden and Cole, causing concerns amongst marijuana businesses and consumers.[28] Under the Trump Administration, Attorney General Jeff Sessions stated that, "marijuana is not the kind of thing that ought to be legalized."[29] At his confirmation hearing, he continued to voice his strong opposition to marijuana legalization, and indicated that federal enforcement of marijuana related activities were imminent.[30] Sessions issued a memo in the beginning of 2018 stating that "previous nationwide guidance specific to marijuana enforcement is unnecessary and is rescinded, effective immediately."[31] The Sessions memo generated public concern about the possibility of a crackdown on the marijuana industry in the United States.[32] Consequently, consumers grew worried about purchasing the classified Schedule 1 drug and potentially facing legal consequences.[33]

This fear manifested in an attempt of California to pass legislation prohibiting state law enforcement authorities from cooperating with federal authorities in certain marijuana

---

[27] *See* Fourth Corner Credit Union v. Fed. Reserve Bank of Kansas City, 154 F. Supp. 3d 1185, 1189 (D. Colo. 2016), vacated, 861 F.3d 1052 (10th Cir. 2017).
[28] Tom Angell, *Stop Jeff Sessions From Busting Medical Marijuana, Bipartisan Lawmakers Demand*, FORBES (Mar. 16, 2018), https://www.forbes.com/sites/tomangell/2018/03/16/stop-jeff-sessions-from-busting-medical-marijuana-bipartisan-lawmakers-demand/#27bf70621a74.
[29] Tom Huddleston, Jr., What Jeff Sessions Said About Marijuana in His Attorney General Hearing, FORTUNE, (Jan. 10, 2017), http://fortune.com/2017/01/10/jeff-sessions-marijuana-confirmation-hearing/
[30] *Id.*
[31] Memorandum from Jefferson B. Sessions III, Att'y Gen. to U.S. Attorneys, Marijuana Enforcement, (Jan. 4, 2018).
[32] Patrick McGreevy, Weed's Legal in California, But Activists Fear a Battle Ahead with Jeff Sessions - Trump's Pick for Attorney General, L.A. TIMES (Dec 1, 2016, 12:05 AM), http://www.latimes.com/politics/lapol-ca-marijuana-legalization-jeff-sessions-snap-20161201-story.html
[33] *Id.*

investigations.[34] Specifically, AB 1578 would prohibit a state agency "from using agency resources to assist a federal agency to investigate, detain, detect, report, or arrest a person for marijuana activity that is authorized by law in the State of California and transferring an individual to federal law enforcement authorities for purposes of marijuana enforcement."[35] Unless, however, a court order directed Californian authorities to do so.[36] Furthermore, the California bill would have prohibited "a state or local agency . . . [from providing] information about a person who has applied for or received a license to engage in commercial marijuana or commercial medical cannabis activity pursuant to MCRSA or AUMA, if the request is made for the purposes of enforcing the . . . Controlled Substances Act."[37]

There are also non-financially related concerns with purchasing marijuana. Many consumers who purchase and use marijuana legally are concerned about the stigma associated with the "schedule 1 drug."[38] A study of medical marijuana users in California revealed that "stigma emerged as a primary and recurring issue as it related to both the process of becoming a medical marijuana user, and remaining one."[39] Adding to the stigma were remarks by Sessions about marijuana consumers: "good people don't smoke marijuana."[40] Marijuana consumers are thus not inclined for their personal data to be associated with marijuana consumption.

---

[34] *See* ASSEMBLY COMMITTEE ON PUBLIC SAFETY, COMMITTEE ANALYSIS OF AB 1578 (Apr. 18, 2017) ("Over 60% of American support legalizing cannabis but U.S. Attorney General Jeff Sessions is still stuck in the Reefer Madness era … This unwarranted federal crackdown not only undermines state autonomy … but also is a misguided waste of public resources …").
[35] *Id.*
[36] *Id.*
[37] SENATE COMM. ON PUB. SAFETY, MARIJUANA AND CANNABIS PROGRAMS: COOPERATION WITH FEDERAL AUTHORITIES (June 27, 2017).
[38] Joan L. Bottorf ET AL., *Perception of Cannabis as a Stigmatized Medicine: A Qualitative Descriptive* Study, 10 HARM REDUCTION J. 2 (2013).
[39] Travis Satterlund ET AL., *Stigma Among California's Medical Marijuana Patients*, 47 J. PSYCHOACTIVE DRUGS 1 (2016).
[40] *See* Alec Siegel, *Could California Become a Sanctuary State for Marijuana Business?*, LAWSTREET MEDIA (April 4, 2017), https://lawstreetmedia.com/blogs/cannabis-in-america/california-sanctuary-state/.

B. Legal Marijuana Consumption and the Drug Free Workplace

Pursuant to a business's right to maintain a drug free workplace, an employer can still terminate workers who consume marijuana, even in a state where it is legalized.[41] This remains true even in cases where employees are medically prescribed marijuana.[42] In 2010, a medically licensed marijuana user suffering from quadriplegia was fired from his job at Dish Network LLC ("Dish") for failing a drug test after testing positive for THC (the active ingredient in marijuana).[43] The Colorado Supreme Court affirmed the lower court's dismissal of the suit the employee brought against Dish, explaining that the employee's "use of medical marijuana was unlawful under federal law and thus not protected by Colorado's employment discrimination statute."[44]

The tension between employer drug free workplace policies and legal consumption of marijuana presents problems for both employers and employees; that is, employers are concerned about violating an employee's the right to privacy, and employees face risk of termination for engaging in a completely legal activity.[45] These antagonizing forces have resulted in certain states amending their marijuana laws in various ways.[46] For example, the Illinois legislature recently passed an amendment allowing employers to discipline employees or

---

[41] *See* Emerald Steel Fabricators, Inc. v Bureau of Labor & Indus, 230 P.3d 518 (Or. 2010); Roe v. Teletech Customer Care Mgmt. (Colo.) LLC, 257 P.3d 586 (Wash. 2011); *see also* G.M. Filisko, *Employers and Workers Grapple with Laws Allowing Marijuana Use*, AM. BAR ASS'N J. (Dec. 2015), http://www.abajournal.com/magazine/article/employers_and_workers_grapple_with_laws_allowing_marijuana_use

[42] *See* Coats v. Dish Network, LLC, 350 P..3d 849 (Colo. 2015); *see also* Beinor v. Indus. Claim Appeals Office of Colo. & Serv. Grp., Inc., 262 P.3d 970 (Colo. App. 2011) (Involving the termination of an employee who tested positive for marijuana, violating the employer's zero-tolerance drug policy. Even though the employee was a medical marijuana user as per Colo. Const. art. XVIII, § 14, and only used marijuana outside of work, the employee was lawfully denied unemployment compensation benefits.)

[43] *Id.* at 850.

[44] *Id.* at 852-53.

[45] Nathaniel Glasser & Eric Emanuelson, *Puff, Puff, Passed: 2019 Marijuana Laws in Review and 2020 Projections*, INSURANCE JOURNAL (Dec. 31, 2019), https://www.insurancejournal.com/news/national/2019/12/31/553137.htm

[46] *Id.*

refuse employment to applicants who violate an Illinois business's drug policy.[47] The amendment states that "nothing in this Act shall prohibit an employer from adopting reasonable zero tolerance or drug free workplace policies, or employment policies concerning drug testing," as long as it is done in an non-discriminatory manor.[48]

However, other states have taken a different approach than Illinois by expanding protection for employees who consume marijuana.[49] On January 1, 2020, a new law went into effect in Nevada prohibiting employers from refusing to hire potential employees because the employee tested positive for marijuana.[50] In passing Int. 1445-A, New York City went as far as preventing employers from administering drug tests on prospective employees.[51] Many other states, including New Mexico and Oklahoma, have passed legislation protecting medical marijuana employees, but not all states have followed suit.[52]

Until all states where marijuana consumption is recreational consumption is legal have provided legal protection to employees who consume marijuana, consumers will remain weary of how their data is being collected by marijuana businesses.

II. Data Privacy

A. Tension Between the Value of Data and Consumer Protection

[47] State Officials and Employment Ethics Act, 5 ILL. COMP. STAT. ANN. 430/5-45 (West 2020).
[48] *Id.*
[49] Glasser, *supra* at note 45.
[50] *Id.*
[51] *Id.* (However, "the ordinance provides several exceptions to allow drug testing of applicants for safety-related positions, transport-related positions, caregivers, and certain federal contractors.)
[52] *Id.*

A 2017 issue of *The Economist* called "data" the most valuable resource in the world.[53] According to a survey conducted by PricewaterhouseCoopers, "[d]ata will be the most important consideration in 2019 and that consumer data is the most valuable for companies to harvest."[54] Companies view personal data as a corporate asset, and a commodity, one of which companies seek to monetize and generate substantial profits from.[55]

In the context of bankruptcy proceedings, companies can sell off their consumer bases for exorbitant sums. For example, in 2016, Dick's Sporting Goods bought 114 million customer files and 25 million email addresses for $15 million when Sports Authority, Inc. filed for Chapter 11 bankruptcy.[56] The ability for companies to sell this information in bankruptcy proceedings is largely contingent on their privacy policies.[57] In 2015, "RadioShack filed for bankruptcy and among the company's assets were "117 million customer records" that included personally identifiable information, such as dates of birth, credit and debit card numbers, names, and physical and email addresses."[58] However, RadioShack had a more consumer friendly privacy policy than Sports Authority.[59] RadioShack's website specifically stated, "we will not sell or

---

[53] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1371 (2017) (citing *Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data*, Economist (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource).

[54] Andrew Busby, *New PwC Survey Reveal Consumer Data is the Most Highly Valued*, FORBES (March 4, 2019), https://www.forbes.com/sites/andrewbusby/2019/03/04/new-pwc-survey-reveals-consumer-data-is-the-most-highly-valued/#7729b971640c.

[55] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV 2056, 2056-57 (2004) ("The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend.").

[56] Kathryn Rattigan, *Sports Authority Sells its Customer Database to Dick's Sporting Goods for $15 Million*, DATA PRIVACY + SECURITY INSIDER BLOG (July, 7, 2016), https://www.dataprivacyandsecurityinsider.com/2016/07/sports-authority-sells-it-customer-database-to-dicks-sporting-goods-for-15-million/.

[57] *See generally*, Michael St. Patrick Baxter, *The Sale of Personally Identifiable Information in Banktruptcy*, AM. BANKR. INST. L. REV. 1 (discussing the implications of a company's privacy policy in the context of bankruptcy proceedings).

[58] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 431 (2017).

[59] *Id.*

rent your personally identifiable information to anyone at any time." [60] Thus, since RadioShack did not contain a carve out in its privacy policy with regards to bankruptcy proceedings, it was restricted from selling much of its consumer data.[61] It is also common for companies to change their privacy from a more restrictive to less restrictive over the life course of the business.[62]

A company looking to maximize the value of their assets might not be inclined to provide comprehensive privacy protection to its consumers.[63] Consumers need not worry too much because marijuana related businesses are largely limited when filing for bankruptcy,[64] but a recent Ninth Circuit ruling demonstrated that not all bankruptcy courts will shut their doors on such businesses.[65] A New York Times report analyzing the top 100 websites in the United States found that over eighty-five percent "said they might transfer users' information if a merger, acquisition, bankruptcy, asset sale or other transaction occurred."[66]

---

[60] Michael Hiltzik, *The RadioShack Bankruptcy Shows You Can't Trust a Company's Privacy Pledge*, L.A. TIMES (May 19, 2015), https://www.latimes.com/business/la-fi-mh-radioshack-you-have-no-privacy-left-20150519-column.html.

[61] Elvy, supra **Error! Bookmark not defined.** at 422-23. *See also* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 783 (2016) (noting that "RadioShack's privacy policy . . . [provided] that consumers' data would not be sold, or, alternatively, that RadioShack would obtain consumers' affirmative consent before transferring their personal data," and that, ultimately, RadioShack "agree[d] to destroy most of the data, including Social Security numbers, telephone numbers, and dates of birth, and to reduce the number of data points per customer available for sale from 170 to 7").

[62] *See* Baxter, supra note 57, at 9.

[63] *Id.*

[64] *See e.g.*, In re Arenas, 514 B.R. 887 (Bankr. D. Colo. 2014) (concluding a legal marijuana producer was precluded from utilizing the bankruptcy code); *see also* In re Rent-Rite Super Kegs W. Ltd., 484 B.R. 799 (Bankr. D. Colo. 2012) (dismissing a case where a debtor who derived 25% of its revenues from leasing warehouse space to marijuana growers was found in violation Controlled Substances Act).

[65] *See* Garvin v. Cook Invs., 922 F.3d 1031, 0136 (9th Cir. 2019) (confirming the Chapter 11 plan of a company that leased their facilities to marijuana producers); *see also* Keith Owens, *Distressed Cannabis Companies See Hope in 9th Circ. Ruling*, LAW360 (May 22, 2019) (discussing the possible implications of the ruling in Cook v. Garvin Invs.).

[66] Natasha Singer & Jeremy B. Merrill, *When a Company Is Put Up for Sale, in Many Cases, Your Personally Data Is, Too*, N.Y. TIMES (June 28, 2015), https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html.

This sort of risk and uncertainty does not sit well with consumers.[67] Recent surveys show a majority of consumers are concerned about their data being sold to third parties.[68] According to a study conducted by Pew in 2016, over one-third of surveyed consumers are not confident that companies and retailers they do business with will protect their data.[69] The study also found "that a majority of the public has noticed or been notified of a major data breach impacting their sensitive accounts or personal data."[70] Consumer discontent towards data collection is substantiated by various threats posed when companies solicit and hold on to their data.[71] These include, "data breach, internal misuse unwanted secondary use, government access, and chilling effect on consumer behavior."[72] This discontent is amplified when consumers are purchasing marijuana.

B. Data Privacy Law in the United States

Data privacy law, also known as "information privacy law," refers to the "collection, use, and disclosure of personal data."[73] In the United States, citizens are not afforded a constitutional right to information privacy.[74] The Supreme Court has ruled that "the Constitution does not protect the individual when a "third party," such as her bank, surrenders her personal information

---

[67] *See* JESSICA GROOPMAN & SUSAN ETLINGER, CONSUMER PERCEPTIONS OF PRIVACY IN THE INTERNET OF THINGS, , ALTIMETER 2 (June 2015) (finding 78% of consumers are highly concerned about companies selling their data to third parties).
[68] *Id.*
[69] Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CENTER (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.
[70] *Id.*
[71] *See, e.g.*, Justin Brookmen & G.S. Hans, WHY COLLECTION MATTERSL SURVEILLANCE AS A DE FACTO PRIVACY HARM 2, CTR. FOR DEM. & TECH. (Sep. 30, 2013), *available at* https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.
[72] *Id.*
[73] Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text* 3 (Geo.Wash. U. L. Sch., Research Paper No. 2019-67, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3457563
[74] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 132 (2017).

to the government."[75] Rather, constitutional protections favor the free flow of data, as opposed to ensuring safeguards for personal data privacy.[76]

At the federal level, the United States lacks a comprehensive framework protecting the collection and use of consumer data.[77] Instead, the United States has implemented "patchwork" protections consisting of the regulation of different sectors, such as the health industry via the Health Insurance Portability and Accountability Act ("HIPAA").[78] Because of this sector based approach, consumers are only afforded limited federal statutory protection.[79] Some federal privacy acts include: the Children's Online Privacy Protection Act ("COPPA") (protecting the information of Children on the internet);[80] the Stored Communications Act ("SCA") (prohibiting unauthorized access of communications held by internet service providers);[81] and the Gramm-Leach-Bliley Act (regulating the protection of the use of personal information of individuals by financial institutions).[82]

The Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices, provides limitations to how companies handle personal data.[83] The Federal Trade Commission ("FTC") regulates poor data security practices by companies under Section 5 of the FTC Act,

---

[75] *Id.* at 133 (citing Smith v. Maryland, 442 U.S. 735 (1979)).
[76] *Id.* at 134.
[77] Nuala O'Conner, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection;
[78] *See* The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; *see* 45 C.F.R. Parts 160, 162, & 164 for regulations about privacy. *See also* The Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted under the American Recovery and Reinvestment Act of 2009, Div. A, Title XIII of Pub. L. 111-5.
[79] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 5, 6 (2012).
[80] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2006).
[81] Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1212 (2004) ("The [SCA] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.").
[82] 15 U.S.C. §§6801-6809 (2012).
[83] 15 U.S.C. § 45(a) (2006).

which provides that "the Commission is hereby empowered and directed to prevent persons, partnerships, or corporations … from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[84]

However, the FTC evaluates companies' data security practices on a case by case basis and will not always pursue a company for inadequate data security practices.[85] For the FTC to bring a successful unfairness claim against a company, it has to prove that the act or practice: (1) causes or is likely to cause a substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves, and (3) not outweighed by countervailing benefits to consumers or competition.[86] Generally, most companies end up settling when the FTC brings an Action against them,[87] but, recently, Wyndham Worldwide Corp. challenged the authority of the FTC as a regulator of data security, which resulted in a case before the United States District Court in New Jersey.[88]

It is unclear how, and if, the FTC regulates marijuana businesses' data security practices. The FTC is a federal agency,[89] and, as explained above, marijuana is prohibited by federal law.[90] The federal government generally allows marijuana businesses access to federal resources and institutions,[91] and I am not aware of an instance where the FTC has interacted with a marijuana business regarding its data security practices.[92]

---

[84] *Id.*
[85] *See* Wyndham, infra note 88.
[86] 15 U.S.C. § 45(n).
[87] *See* Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. 583, 606-07 (2014).
[88] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).
[89] 15 U.S.C. § 45(a) (2006).
[90] Controlled Substances Act, 21 U.S.C.S. § 812.
[91] *See, e.g.*, In re Arenas infra note 64 (discuss marijuana and bankruptcy).
[92] *But cf.*, Press Release, Federal Trade Commission, FTC Sends Warning Letters to Companies Advertising Their CBD-Infused Products as Treatments for Serious Diseases, Including Cancer, Alzheimer's, and Multiple Sclerosis (Sept. 10, 2019) (on file with author).

A lack of comprehensive federal protection for data privacy of individuals has pushed states to start passing their own data privacy legislation.[93] The courts generally serve to regulate data protection in states through tort and contract law.[94] In the context of tort law, negligence and similar claims regulate companies that "fail to protect their customers from foreseeable harm."[95] Although, this avenue is not available in every state.[96] Contract law also serves as important protection mechanism affording redress to victims involving privacy issues.[97] Many states have passed consumer protection acts (CPAs) which provide consumers with private rights of actions mentioned above, which is not afforded to persons under the FTC.[98]

Initially, states attempted to ameliorate the patchwork approach to data privacy at the federal level by passing data breach notification laws. Prior to turn of the twenty-first century, companies were not legally obligated to provide notice to consumer of a data breach.[99] In 2003, California became the first state to pass a breach notification law.[100] Currently, in 2019, all fifty

---

[93] Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html

[94] STEPHEN P. MULLIGAN ET AL.., CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 30 (2019).

[95] MULLINGAN, *supra* 12, at 30 (2019) (citing Anderson v. Hannaford Bros. Co., 659 F.3d 151, 161–62 (1st Cir. 2011) (concluding that plaintiffs had adequately stated claim for negligence against grocer when payment data was allegedly stolen by third party wrongdoer)).

[96] *See* USAA Federal Savings Bank v. PLS Financial Services, Inc., 260 F. Supp. 3d 965, 969–70 (N.D. Ill. 2017) (holding that Illinois law did not recognize a common law duty to safeguard personal information); Target, 66 F. Supp. 3d at 1176 (concluding that "economic loss rule" barred negligence claims under the laws of several states); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 564, 822-29 (6th ed. 2018) (discussing obstacles to using tort law to remedy privacy harms).

[97] *See* MULLIGAN, supra note 94, at 37 (citing Hutton v. National Board of Examiners in Optometry, Inc., 892 F.3d 613, 623–24 (4th Cir. 2018) (concluding that plaintiffs had standing to assert claims arising out of breach of personal information database, including breach of contract); Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1246–48 (D. Colo. 2018) (concluding that plaintiffs had adequately pleaded claim for breach of implied contract in case involving data breach and theft of personally identifiable information)).

[98] Victor E. Schwartz & Cary Silverman, Common-Sense Construction of Consumer Protection Acts, 54 U. Kan. L. Rev. 1, 3 (2005).

[99] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 767 (2016).

[100] Cal. Civ. Code § 1798.29, 1798.82 (effective through 2020); *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 189 (5th ed. 2019) (describing "California's Data Security Breach Notification Statute").

states have some form of a data breach notification law.[101] These laws vary greatly from state to state,[102] and change routinely.[103]

Critics argue that data breach notification laws, however, are not a perfect solution to comprehensive data privacy protection.[104] The lack of uniformity amongst these laws makes it difficult for consumers to understand when, where, and how they are being protected.[105] For example, initially Florida and California were the only states that required consumers to be notified when their email address and password became compromised; most states lacked this requirement, but some have since followed Florida and California's approach.[106] Additionally, some states require that the attorney general bring an action if a company violates a data breach notification law, but, in other states, the law allows private citizens to bring an action if a harm is resulted from the breach.[107]

These laws also vary in the way they define personal information, the amount of time in which an individual or entity is notified when a breach occurs, and if notification is even required because of the scope of the breach involved.[108] Even more troubling is that most

---

[101] For a chart of each state's data breach notification law, *see* STATE DATA BREACH NOTIFICATION LAWS, FOLEY & LARDNER LLP (Oct. 25, 2019), *available at* https://www.foley.com/-/media/files/insights/publications/2019/11/19mc23532-data-breach-chart-update-101419.pdf.
[102] O'Connor, supra note 77.
[103] *See e.g.*, Brian Kint & Cozen O'Conner, *Year to Date Change to State Data Breach Notification Laws*, JDSUPRA (July 22, 2019), https://www.jdsupra.com/legalnews/year-to-date-changes-to-state-data-21648/ (discussing the changes to in various state data breach notification laws in 2019).
[104] *See generally*, Jaikumar Vijayan, *Critics Hit Proposed Data Breach Notification Laws as Ineffective*, COMPUTERWORLD (Nov. 10, 2005), https://www.computerworld.com/article/2558781/critics-hit-proposed-data-breach-notification-law-as-ineffective.html
[105] *See* Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1185 (2014) (discussing that confusion caused by varying data breach notification laws).
[106] *See* Joseph J. Lazzarotti ET AL., *State Data Breach Notification Laws: Overview of the Patchwork*, JACKSON LEWIS (April 9, 2018), *available at* https://www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork.
[107] *Id.*
[108] *See* State Data Breach Notification Law Chart, supra note 101.

statutes include safe harbor provisions that shield companies from liability when the breached data was encrypted.[109] Compliance in each state varies as well, and things become more complicated when data breaches reach outside the borders of the state where the company is operating.[110] Furthermore, data breach notification laws only become effective *after* a breach has transpired and an individual's personal information has been compromised; by that point, the harm to the individual has already occurred.[111]

C. The California Consumer Privacy Act

In the past few years, states began approaching data privacy law more aggressively than they have done in the past by attempting to enact comprehensive privacy legislation that goes beyond their breach notification laws.[112] As a pioneer in the field of data privacy, California has led efforts in the trend to provide greater privacy protection to consumers.[113] In 2018, California passed the California Consumer Privacy Act ("CCPA"), which is considered by most experts as the most comprehensive form of privacy protection by a state.[114] California's Act draws substantial influence from the European Union's General Data Protection Regulation ("GDPR").[115] The Act begins by stating, "The California Constitution grants a right of privacy."[116] Within this right of privacy, Californians will be afforded: (1) the right "to know what personal information is being collected about them;"[117] (2) the right "to know whether their

---

[109] *See* Alice M. Porch, *Safe Harbor From Data Breach Notification*, CYBER L. BLOG (July 3, 2017), https://www.amp.legal/blog/safe-harbor-from-data-breach-notification/
[110] *See* Peters, supra note 105, at 1183-85 (discussing compliance issues with state data breach notification laws).
[111] *See generally* State Data Breach Notification Law Chart, supra note 101.
[112] Footnote Needed
[113] See John Myers & Jazmine Ulloa, *California Lawmakers Agree to New Consumer Privacy Rules that Would Avert Showdown on the November Ballot*, L.A. Times (June 21, 2018), https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.
[114] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100 (West 2018)
[115] *See* Paul M. Schwartz, *Symposium: Global Data Privacy: The EU Way*, 94 N.Y.U.L REV. 771, 817 (2019).
[116] § 1798.100.
[117] *Id.*

personal information is sold or disclosed and to whom;"[118] (3) the right "to say no to the sale of personal information;"[119] (4) the right to access their personal information;"[120] and (5) the right "to equal service and price, even if they exercise their privacy rights."[121]

The CCPA also affords consumers the right to request that businesses delete the consumer's personal information, more commonly known as 'the right to be forgotten.'[122] However, the Act has a carveout allowing businesses to hold onto the consumer's personal information for a list of reasons, including to "comply with a legal obligation."[123]

California's Act has its limitations. The CCPA only applies to companies that meet one of the following three criteria: (1) the business generates at least $25 million in annual revenue;[124] (2) the business "alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;"[125] or (3) derives at least half of "its annual revenues from selling consumers' personal information."[126] Furthermore, although the CCPA grants consumers a right "to equal service and price, even if they exercise their privacy rights," the CCPA contains a provision that seems to undermine this right. It states that "[n]othing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the

---

[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100 (West 2018)
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Id.* (The act specifically lists 9 scenarios that allow a business to disregard a consumer's request to be forgotten.)

consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data."

It remains unclear how the CCPA will impact marijuana businesses.[127] Many marijuana businesses do not meet the annual revenue threshold, nor do they derive fifty percent of their revenue from selling the personal information of consumers.[128] But, marijuana businesses might check off the third criteria – a business that buys, sells, receives, or shares the personal information of 50,000 or more consumers.[129] A guidance document recently prepared for the Attorney General's Office predicts that "either fifty percent or seventy-five percent of all California business that earn less than $25 million will be covered under the CCPA."[130] Nevertheless, the CCPA will force marijuana businesses to take greater measures ensuring they are in compliance with the new California law.[131]

Nevada, New York, Washington, and Texas are all expected to roll out similar legislation to the CCPA in the next few years that would provide a comprehensive data protection scheme for their respective states.[132]

---

[127] Scott Bloomberg, *California, Cannabis and Data Privacy*, JDSUPRA (Sept. 5, 2019), https://www.jdsupra.com/legalnews/california-cannabis-and-data-privacy-52009/

[128] *See* Griffin Thorne, *A New California Law Will Affect Marijuana and Hemp Businesses Across the Nation*, CANNA LAW BLOG (Nov. 9 2019), https://www.cannalawblog.com/a-new-california-law-will-affect-marijuana-and-hemp-businesses-across-the-nation/; see also Daniel R. Stoller, *California Pot Firms Aim to Deliver Privacy Weed Users Want*, BLOOMBERG LAW (Feb. 28, 2020) ("Much of California's pot industry likely falls short of the revenue figure that would require compliance."), https://news.bloomberglaw.com/privacy-and-data-security/california-pot-firms-aim-to-deliver-privacy-weed-users-want

[129] *Id.*

[130] BERKLEY ECONOMIC ADVISING AND RESEARCH, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 20 (August 2019), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

[131] *See* David Strauss, *Analyzing the California Consumer Privacy Act's Impact on the Cannabis Industry*, CANNABIS LAW NOW (Mar. 7, 2019), https://www.cannabislawnow.com/2019/03/analyzing-the-california-consumer-privacy-acts-impact-on-the-cannabis-industry/

[132] *See* Jeewon Kim Serrato & Susan Ross, *Nevada, New York and Other States Follow California's CCPA*, DATA PROTECTION REPORT (Jun. 6, 2019), https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/

III. Legal Analysis

A. Data Privacy Protection and Concerns for Legal Consumers of Marijuana

The California Consumer Privacy Act and other similar pending legislation by states are provide represent an impressive milestone in United States data privacy law, however, some gaps may leave the personal data of marijuana consumers vulnerable.[133] Many questions are left unanswered. That is, do these acts sufficiently appease the concerns of legal purchasers of marijuana? Or, are they not specific enough to alleviate the apprehension of their personal data falling into the wrong hands?

In the first half of 2018 alone, approximately 4.5 billion records were exposed due to data breaches.[134] Out of a multitude of legal concerns for marijuana businesses, "data breaches are the most likely thing that will occur."[135] Because of the illegality of marijuana at the federal level, marijuana businesses might be less likely to report a breach if it were to occur.[136] For the same reason, marijuana businesses might employ sub-par electronic banking sources, exposing them to potential data breaches.[137]

THSuite, which calls itself "the trusted software partner for the cannabis industry,"[138] provides marijuana dispensary owners and operators with point-of-sale system solutions.[139] In December 2019, the company fell victim to a data breach, which was discovered by two internet

---

[133] Footnote Needed
[134] Griffin Thorne, *Cannabis Companies Are Overlooking Data Security Laws and Regulations*, JURIST.ORG (Mar. 17, 2020), https://www.jurist.org/commentary/2020/03/griffen-thorne-ccpa-cannibas/
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] THSuite, LINKEDIN, https://www.linkedin.com/company/thsuite (last visited April 10, 2020).
[139] *Id.*

privacy researchers unrelated to the company.[140] Almost three weeks lapsed between the date the owners of THSuite were notified of the breach and the date THSuite closed the exposed database.[141] Over 85,000 files were leaked during this breach, which included personal information of over 30,000 customers, such as full name, phone number, email address, date of birth, and street address.[142]

A breach, such as the recent one with THSuite, has far-reaching consequences for consumers and businesses. Consumer confidence is weakened, and customers are less-likely to give business to marijuana dispensaries and other related entities that are unable to adequately secure their personal information.[143] Furthermore, companies suffering a breach are potentially exposed to significant penalties, and even possibly jail time, depending on the state in which the breach occurred and who suffered.[144]

Thus, state legislation limiting marijuana businesses from collecting and retaining personal information is important to prevent data breaches from occurring and as well as mitigating the effects of a breach if and when it occurs.

B. States' Approach to Marijuana Legislation and Data Privacy

There are roughly three categories describing the way states have implemented data privacy protection in their marijuana legislation; these categories are not mutually exclusive.

---

[140] *Report: Cannabis User's Sensitive Data Exposed in Data Breach*, VPNMENTOR (Jan. 24, 2020), https://www.vpnmentor.com/blog/report-thsuite-breach/.
[141] *Id.*
[142] *Id.*
[143] Matthew R. Kittay & Alexander Kerzhner, *Data Breach Exposes Cannabis Industry Security Vulnerabilities*, FOX ROTHSCHILD (Feb. 25, 2020), https://www.foxrothschild.com/publications/data-breach-exposes-cannabis-industry-security-vulnerabilities/.
[144] *Id.*

The first category involves a scenario where the state's original piece of legislation authorizing marijuana use has a data privacy provision included. The second category is where the state has passed supplemental marijuana-related legislation specifically focusing on data privacy. And the third category is one where a state that has legalized marijuana contains no related data privacy legislation at all.

Colorado, one of the initial states to legalize marijuana recreationally, falls into the first category.[145] Colorado amended its Constitution via Proposition 64 to authorize the recreational use of marijuana in 2012.[146] This amendment contained a data privacy provision pertaining to marijuana businesses.[147] The provision reads:

> In order to ensure that individual privacy is protected … the Department shall not require a consumer to provide a retail marijuana store with personal information other than government-issued identification to determine the consumer's age, and a retail marijuana store shall not be required to acquire and record personal information about consumers other than information typical acquired in a financial transaction conducted at a retail liquor store.[148]

The phrase "shall not require" is common throughout several states' marijuana legislation.[149] The troubling aspect of this phrase is that it essentially serves no practical purpose; when a privacy agreement says "shall not require" it is actually permitting the business to collect personal data. And, depending on the state's data protection laws, this could result in a business collecting personal data unrestrictedly. As demonstrated earlier in this paper, businesses are incentivized to

---

[145] Keith Coffman & Nicole Neroulias, *Colorado, Washington First States to Legalize Recreational Pot*, REUTERS (Nov. 6, 2012, 7:53 PM), https://www.reuters.com/article/us-usa-marijuana-legalization/colorado-washington-first-states-to-legalize-recreational-pot-idUSBRE8A602D20121107.
[146] COLO. REV. STAT. ANN. COLO. CONST. ART. XVIII, § 16 (Use and Regulation of Marijuana) (West 2018).
[147] *Id.*
[148] *Id.*
[149] *See, e.g.*, Cannabis Regulation and Tax Act, 410 ILL. COMP. STAT. ANN. 705/1 (West 2020).

collect personal data of consumers because of the substantial value it possesses.[150] For example, many marijuana dispensaries have marketing schemes and rewards programs that utilize a consumer's personal data.[151] Alternatively, businesses might over collect data in an effort to be compliant with regulations.[152]

Illinois also falls into the first category with Colorado. Illinois was the most recent state to legalize marijuana for recreational use.[153] It is also the first state to legalize the adult use of marijuana through the legislative process, as opposed to a ballot initiative seen by prior states.[154] However, Illinois's Cannabis Regulation and Tax Act contains the strongest privacy provision out of any state's initial marijuana legislation.[155] Regarding data privacy, the Act reads:

> To protect personal privacy, the Department of Financial and Professional Regulation shall not require a purchaser to provide a dispensing organization with personal information other than government-issued identification to determine the purchaser's age … and a dispensing organization shall not obtain and record personal information about a purchaser without the purchaser's consent…Any identifying or personal information of a purchaser obtained or received in accordance with this section shall not be retained, used, shared, or disclosed for any purpose except as authorized by this Act.[156]

Although Illinois's Act contains the permissive phrase "shall not require," it clarified that a marijuana dispensary can only obtain the personal information of a consumer with his or her

---

[150] *See* Busby, supra note 54
[151] *See* S.B. 863, Leg. Assemb., Reg. Sess. (Or. 2017) ((5)(A) NOTWITHSTANDING SUBSECTION (3) OF THIS SECTION, A MARIJUANA RETAILER MAY RECORD AND RETAIN THE NAME AND CONTACT INFORMATION OF A CONSUMER FOR THE PURPOSE OF NOTIFYING THE CONSUMER OF SERVICES THAT THE MARIJUANA RETAILER PROVIDES OR OF DISCOUNTS, COUPONS AND OTHER MARKETING INFORMATION IF…)
[152] *See* Electronic Frontier Foundation, infra note 176.
[153] Vincent Caruso & Austin Berg, *Illinois Becomes 11th State to Legalize Recreational Marijuana*, ILLINOIS POLICY (June 25, 2019), https://www.illinoispolicy.org/illinois-becomes-11th-state-to-legalize-recreational-marijuana/
[154] *Id.*
[155] Cannabis Regulation and Tax Act, 410 ILL. COMP. STAT. ANN. 705/1 (West 2019).
[156] *Id.*

consent, operating like an opt-in feature.[157] This provision was missing from Colorado's legislation mentioned above.[158]

Illinois's legislation also adds an extra layer of protection to consumers in the context of employment.[159] It amends the Right to Privacy in the Workplace Act by prohibiting employers from discriminating against an employee who uses "lawful products (including marijuana) off the premises of the employer during nonworking and non-call hours."[160] However, this provision is not applicable to all businesses, including some non-profits.[161] Illinois's law plans to go into effect on January 1, 2020.[162]

Alaska is another state that falls into category 1.[163] Alaskans voted for the recreational use of marijuana in 2014 via Measure 2.[164] Similar to Colorado, Alaska's privacy provision in the legislation only states that retailers shall not be required to collect a consumer's personal information, but contains nothing prohibiting retailers from doing so.[165]

Oregon and California are examples of states that fall into the second category mentioned above; that is, states that have passed bills regarding data privacy and marijuana as a reactionary measure to inadequate protections in their original legislative acts.[166] Oregon's original

---

[157] *Id.*
[158] COLO. REV. STAT. ANN. COLO. CONST. ART. XVIII, § 16 (Use and Regulation of Marijuana) (West 2018)
[159] Dale Deitchler ET AL., *Illinois Poised to Protect Marijuana Users from Adverse Employment Actions as Part of Marijuana Legalization Legislation*, JDSUPRA (June 20, 2019), https://www.jdsupra.com/legalnews/illinois-poised-to-protect-marijuana-76364/.
[160] *Id.*
[161] *Id.*
[162] *Id.*
[163] ALASKA STAT. § 17.38.020 (West 2019)
[164] *See* Megan Edge & Laurel Andrews, *Timeline: Notable Moments in 40 Years of Alaska's History with Marijuana*, ANCHORAGE DAILY NEWS (Sep. 28, 2016), https://www.adn.com/cannabis-north/article/alaska-weed-history/2014/04/14/.
[165] ALASKA STAT. § 17.38.020 (West 2019)
[166] 2018 Cal ALS 583, 2018 Cal AB 2402, 2018 Cal Stats. ch. 583; Adult and Medical Use of Cannabis Act, OR S.B. 863 (2017).

marijuana legislation did not contemplate the privacy issues facing recreational marijuana consumers.[167] State Representative Carl Wilson, a sponsor of the bill adding greater privacy protection to Oregon marijuana consumers, noticed the deficiencies in the original legislation.[168] He stated, "the law currently does not prohibit a retailer from retaining additional information about their customers."[169] Rep. Wilson also explained that a driving force behind the bill was the potential crackdown by Sessions on the marijuana industry.[170] The new Oregon bill, SB 863, that amended the legalization act, says that "[a] marijuana retailer may not record and retain any information that may be used to identify a consumer."[171] Additionally, SB 863 prohibits marijuana retailers from transferring "any information that may be used to identify a consumer to any other person."[172] SB 863 also required that, within thirty days of its passing, marijuana retailers destroy any personal information of consumers that they had on file.[173]

Following Oregon's lead, California passed AB 2402 in 2018.[174] Assemblyman Evan Low introduced the bill, to prevent "nefarious businesses … from profiting off the exploitation of consumer privacy."[175] The Electronic Frontier Foundation ("EFF"), a nonprofit organization focused on defending digital privacy rights, sent a letter to Assemblyman Lowe voicing their support of the Bill.[176] The letter expressed the concerns of consumers that marijuana

---

[167] *See* Chris Lehman, *Data on Oregon's Marijuana Users Headed for Greater Protection*, OPB (Apr. 10, 2017),
[168] *Id.*
[169] *Id.*
[170] *Id.*
[171] 17 OR. REV. STAT. ANN § 475B.220 (West 2017) (Information identifying consumers of recreational cannabis; recording, transfer, and use of information).
[172] *Id.*
[173] *Id.*
[174] *See* Griffen Thorne, *Breaking News: California Cannabis Businesses Face New Data Privacy Requirements*, CANNA LAW BLOG (Sept. 21, 2018), https://www.cannalawblog.com/breaking-news-california-cannabis-businesses-face-new-data-privacy-requirements/.
[175] Daniel Oberhaus, *California Weed Dispensaries Can Legally Sell Customer Information to Data Brokers*, VICE (Jun. 7, 2018), https://www.vice.com/en_us/article/bj35p4/weed-dispensary-privacy-california-ab2402.
[176] LETTER FOR SUPPORT FOR CALIFORNIA A.B. 2402, ELECTRONIC FRONTIER FOUNDATION (May 25, 2018), *available at* https://www.eff.org/document/letter-california-ab-2402.

dispensaries were over collection consumer personal information.[177] Of those concerns in the letter was that the information, if passed into the wrong hands through a data broker, "could be used to discriminate against lawful cannabis consumers in housing, hiring, credit, and benefits."[178]

The Fresno Bee, a local California newspaper, surveyed several marijuana vendors about their data privacy practices.[179] They found that every single store surveyed kept customer profiles contained personal information of consumers on dispensary computers.[180] These retailers reasoned that they collected the information because it was required by Proposition 64.[181] However, these retailers were incorrect in their interpretation of the legislation—the act specifically said that retailers shall not be required to collect consumer's personal information.[182] Furthermore, some retailers even turned away consumers that were unwilling to give provide their personal information for retention.[183]

Thanks to AB 2402, the aforementioned practices of these vendors are now prohibited by law in California.[184] The Legislative Digest of the A.B. 2402 explains , "[t]he bill would prohibit a licensee from discriminating against a consumer or denying a consumer a product or service because he or she has not provided consent to authorize the licensee to disclose the consumer's

---

[177] *Id.*
[178] *Id.*
[179] Jim Guy, *Recreational Pot Vendors Don't Need to Keep Your Personal Info. But They Do Anyway*, FRESNO BEE (May 24, 2018), https://www.fresnobee.com/news/local/pot-in-california/article211813819.html; *see also* Chris Nichols, *How Much Privacy Do You Have When You Buy Marijuana in California*, POLTIFACT (Feb. 13, 2018, 2:19 PM) (Politifact conducted similar a similar survey to the Fresno Bee. "We found California dispensaries do collect personal information, perhaps more than customers realize. While state law doesn't require this collection, it also doesn't block stores from asking for and retaining it.").
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] CAL. BUS & PROF. CODE § 26161.5 (West 2019) (Added by Stats.2018, c. 583 (A.B.2402), § 1, eff. Jan. 1, 2019.)

nonpublic personal information to a 3rd party not directly related to the transaction." However, this bill is not as aggressive as Oregon's, as for it still collects consumer information.[185] So, if a data breach were to occur, consumers information would be particularly vulnerable.[186]

The third category involves states where there is data privacy provision in any marijuana-related provision. Maine and Washington (state) are two states that fall into this category. Maine legalized marijuana for recreational use in 2016, but the state did not pass legislation setting up a regulatory framework recreational sale until 2019.[187]

Maine's Marijuana Legalization Act makes no mention or reference to personal information or data privacy at all, like most of the other legislation in other states have.[188] The only mention of information is a confidentiality section that reads as follows: "Documents of licensee inspected or examined by the department pursuant to this section are confidential and may not be disclosed except as needed in a civil or criminal proceeding to enforce any provision of this chapter and the rules adopted pursuant to this chapter or any criminal law."[189] However, the act does not define documents to include personal information of customers.[190] Maine did, however, recently sign into law a data protection law protecting online users, but this will provide no relief to legal marijuana consumers.[191] I anticipate that once Maine does finalize the regulation of recreational marijuana sales, they will pass a bill amending current legislation to

---

[185] *Id.*
[186] Unless the business met the requirements of the CCPA. Then they would have to comply with CCPA regulation on storing personal information.
[187] *See* Marina Villenueve, *Janet Mills Signs Bill to Allow Recreational Marijuana Sales in Maine*, BANGOR NEWS DAILY (Jun. 29, 2019), https://bangordailynews.com/2019/06/28/politics/maine-governor-signs-rules-to-finally-allow-pot-sales/.
[188] Marijuana Legalization Act, Me. Rev. Stat. tit. 28-B, § 511.
[189] *Id.*
[190] *Id.*
[191] An Act To Protect the Privacy of Online Customer Information (LD 946, to be codified at 35-A M.R.S. c. 94).

include data privacy protection for marijuana consumers. Similar to what was seen in Oregon and California.

And, although Washington was one of the first states to legalize marijuana recreationally, it does not provide specific data privacy protection to marijuana consumers. [192]

New Jersey and Connecticut have both unsuccessfully tried to legalize marijuana for recreational use.[193][194] New Jersey's Cannabis Regulatory and Expungement Aid Modernization has a provision regarding data privacy, but permits the collection of personal information by retailers, like in Colorado.[195] The Act reads:

> In order to ensure that individual privacy is protected, the commission shall not require a consumer to provide a cannabis retailer with personal information other than government-issued identification to determine the consumer's age, and a cannabis retailer shall not collect and retain any personal information about consumers other than information typically acquired in a financial transaction conducted by the holder of a Class C retail license concerning alcoholic beverages.[196]

It seems as if New Jersey largely styled this provision off Colorado's act; the language is almost identical.

Similarly, Connecticut saw two bills fail pass the first chamber recently. [197] Both bills contained data privacy provisions, but one provided more protection that the other.[198] HB 7371

---

[192] Footnote Needed
[193] Brent Johnson and Susan K. Livio, *Legal Weed Bill for N.J. May Be Revived Later This Year*, NJ.COM (Aug. 7, 2019), https://www.nj.com/marijuana/2019/08/legal-weed-bill-for-nj-may-be-revived-later-this-year-well-make-one-more-run-at-it.html
[194] Rau Hardman, *Why Did the Drive to Make Pot Legal Fail*¸ CT MIRROR (June 13, 2019), https://ctmirror.org/2019/06/12/why-did-the-drive-to-make-pot-legal-fail/
[195] New Jersey Cannabis Regulatory and Expungement Aid Modernization Act., 2018 Bill Text NJ S.B. 2703.
[196] *Id.*
[197] An Act Concerning the Retail Sale of Cannabis, H.B. 7371 (2018); An Act Concerning the Legalization of the Retail Sale and Possession of Cannabis and Concerning Erasure of Criminal Records in the Case of Convictions Based on the Possession of a Small Amount of Cannabis" (S.B. 1085) (2018).
[198] *Id.*

had the common permissive phrase "shall not require" seen in several other states' legislation.[199] However, SB 1085's privacy provision was more consumer friendly.[200] The bill read:

> No cannabis retailed shall (a) electronically or mechanically record or maintain any information from a transaction scan or otherwise obtained from the driver's license or identity card presented by a card holder…(4) no permitee or permitee's agent or employee or cannabis retailer shall sell or otherwise disseminate the information derived from a transaction scan to any third party for any purpose, including but not limited to, any marketing, advertising or promotional activities, except that a permittee or permitee's agent or employee may release that information pursuant to a court order.[201]

The bill allows retailers to record normal identification information but prohibits them from transferring this information to *any* third party.[202] Although it does not goes as far as prohibiting retailers from recording information, like in Oregon, but it does prohibit them from moving this information into a third party's hands; the bill goes beyond California's opt-in provision. Thus, if one of those two bills had passed, consumers would have had vastly disparate effects with regards to data privacy protection.

C. Potential Solutions: A Model Privacy Provision

The best option for marijuana consumers at this point is for states to pass legislation specifically touching the interrelation of data privacy and marijuana purchasing. Illinois's legislation should serve as a model for other states, especially those who have not legalized marijuana recreationally yet, but plan on doing so at some point in the future.[203]

---

[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] Cannabis Regulation and Tax Act, 410 ILL. COMP. STAT. ANN. 705/1 (West 2019).

A model provision can provide clarity for both marijuana businesses and consumers, so that both are aware of what information is being collected, and what information is allowed to be collected, in each respective state where marijuana is legal. Similar to a "model act," which strives to promote uniformity and minimize diversity across jurisdictions, this model provision can serve as a standard for states to adopt retroactively, or incorporate into the drafting of legislation where states plan on legalizing in the near future.[204]

The model provision would read similar to the one in Illinois's legislation: "Any identifying or personal information of a purchaser obtained or received in accordance with this section shall not be retained, used, shared, or disclosed for any purpose except as authorized by this Act."[205] Such a provision can also allow consumers to "opt-in" when purchasing marijuana, if they desire to take part in any rewards program offered by the business. Oregon's legislation is instructive on this point:

> **(a)** Notwithstanding subsection (3) of this section, a marijuana retailer may record and retain the name and contact information of a consumer for the purpose of notifying the consumer of services that the marijuana retailer provides or of discounts, coupons and other marketing information if:
>
> > **(A)** The marijuana retailer asks the consumer whether the marijuana retailer may record and retain the information; and
> >
> > **(B)** The consumer consents to the recording and retention of the information.
>
> **(b)** This subsection does not authorize a marijuana retailer to transfer information that may be used to identify a consumer.[206]

This solution would protect consumers who do not want to risk their personal information being exposed, while allowing businesses to still reap the benefits of commodifying the data of less

---

[204] *What is a Model Act*, UNIFORM LAW COMMISSION, https://www.uniformlaws.org/acts/overview/modelacts
[205] *See* Cannabis Regulation and Tax Act, supra note 155.
[206] [206] 17 OR. REV. STAT. ANN § 475B.220 (West 2017) (Information identifying consumers of recreational cannabis; recording, transfer, and use of information)

wary consumers. Most importantly, the provision allows consumers to be the first line of defense in protecting their personal information.

Marijuana businesses would still have to stay compliant with federal and state regulations, incentivizing owners to employ adequate software and database management to secure their information. Regardless of how strict a potential privacy provision is, businesses still must temporarily collect information for payment purposes if a debit or credit card is involved in the transaction; however, the provision could include a limit on the number of days that the business could store the information.

Conclusion

The ecosystem of data privacy law is an entangled web of patchwork laws affording minimal protection to consumers. And, depending on what state you reside in, there can be hardly any privacy protection at all afforded to legal marijuana consumers.[207] Because marijuana is only legal at the state level, state privacy law will provide the most protection to marijuana consumers. States have begun passing sweeping data privacy legislation, e.g., California's CCPA, but, as demonstrated earlier, these acts might not capture all marijuana businesses, leaving consumers' personal information vulnerable. A model provision, like the one mentioned above, would serve as a useful template for States' to incorporate into marijuana-related legislation, and thus offer consumers vast protection.

[207] *See* Maine's Act, supra note 188.