JOURNAL OF EMERGING ISSUES IN LITIGATION

Tom Hagy
Editor-in-Chief

Volume 1, Number 1
Winter 2021

Editor's Note: From Pot to Privacy to Plastics
Tom Hagy

Clearing the Haze: State Laws and Private Plaintiffs Critical to Preserve Competition in Cannabis
Ausra O. Deluard and Jennifer M. Oliver

Empowering Consumers, California Privacy Laws Could Spell Trouble for Cannabis Companies
Griffen Thorne

Facial Recognition Proliferation: Litigation and Legal Implications of Biometric Technologies
Martin T. Tully and Debbie Reynolds

The Age of Disparagement: How Social Media Has Refueled the Smear
Charlie Kingdollar

Product-Related Privity, Preemption, and the Internet Marketplace
James M. Beck

Crisis Is the Mother of Change: How a Pandemic Sparked Progress in Courtroom Efficiency
Alison Arden Besunder

One Word: Plastics—Two Words: Pollution Exclusion: Why CGL Policies Should Cover Plastics-Related Liabilities
Mikaela Whitman

fastcase FULL COURT PRESS

Journal of Emerging Issues in Litigation

Volume 1, No. 1 Winter 2021

5 **Editor's Note: From Pot to Privacy to Plastics**
Tom Hagy

9 **Clearing the Haze: State Laws and Private Plaintiffs Critical to Preserve Competition in Cannabis**
Ausra O. Deluard and Jennifer M. Oliver

21 **Empowering Consumers, California Privacy Laws Could Spell Trouble for Cannabis Companies**
Griffen Thorne

31 **Facial Recognition Proliferation: Litigation and Legal Implications of Biometric Technologies**
Martin T. Tully and Debbie Reynolds

41 **The Age of Disparagement: How Social Media Has Refueled the Smear**
Charlie Kingdollar

51 **Product-Related Privity, Preemption, and the Internet Marketplace**
James M. Beck

67 **Crisis Is the Mother of Change: How a Pandemic Sparked Progress in Courtroom Efficiency**
Alison Arden Besunder

77 **One Word: Plastics—Two Words: Pollution Exclusion: Why CGL Policies Should Cover Plastics-Related Liabilities**
Mikaela Whitman

JOURNAL OF EMERGING ISSUES IN LITIGATION at $395.00 annually is published four times per year by Full Court Press, a Fastcase, Inc., imprint.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

Cite this publication as:

Journal of Emerging Issues in Litigation (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to JOURNAL OF EMERGING ISSUES IN LITIGATION, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Tom Hagy, Editor-in-Chief, tom.hagy@litigationconferences.com

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

Empowering Consumers, California Privacy Laws Could Spell Trouble for Cannabis Companies

Griffen Thorne*

Abstract: The California Consumer Privacy Act creates private rights of action for Californians that will impact companies regardless of their jurisdiction. The cannabis industry is particularly susceptible to privacy claims; it requires the collection and storage of personal information, but regulations impose little in the way of data protection requirements. This article discusses security controls; potential damages; types of data at risk; other pressures, beyond legal requirements, the industry faces; and mitigation strategies.

The California Consumer Privacy Act (CCPA) is by far the nation's most comprehensive data protection statute. CCPA creates new private rights of action for certain California consumers whose personal information was accessed during a data breach, in the event that the breached company holding their personal information failed to undertake reasonable security measures. CCPA's new private rights of action will have far-reaching effects on companies across the globe.

One industry that will be uniquely susceptible to CCPA litigation is the state's nascent regulated cannabis industry. Under California law, licensed cannabis businesses are required to collect and store a large amount of consumer personal information. However, cannabis regulations generally impose little to no data protection requirements on regulated entities, creating a perfect storm for potential data breaches.

This article examines relevant provisions of CCPA, personal information collection requirements applicable to licensed California cannabis companies, and other unique business and industry pressures applicable to the cannabis industry that will surely lead to future data breaches and CCPA litigation.

Journal of Emerging Issues in Litigation / Winter 2021, Vol. 1, No. 1, pp. 21–30.

CCPA Fundamentals

CCPA was signed into law in 2016, and since then has been the subject of numerous legislative amendments.[1] The law went into effect on January 1, 2020.[2] CCPA is, to date, the nation's most comprehensive general consumer data protection law and is comparable in scope to the European Union's General Data Protection Regulation (GDPR).

At its core, CCPA affords consumers a host of new rights with respect to their data. For example, CCPA provides consumers with the right to request that a company holding their personal information delete that personal information.[3] Many of these rights previously did not exist under California law and generally do not apply to businesses that are not are not regulated under the CCPA.

In addition to affording consumers new legal rights and protections, CCPA also puts the onus on regulated businesses to safeguard personal information. For example, CCPA requires that companies notify consumers about their data collection policies and consumers rights relative to the companies.[4]

In practical terms, this means that CCPA-regulated companies must update their privacy policies and other documents provided to consumers at the point of data collection in order to notify consumers about their new rights and how to exercise them, and for any other information required by law to be disclosed to consumers.[5]

Notably for this article, CCPA augmented existing California data breach notification laws. Under prior California law, companies holding certain important classes of personal information—including Social Security numbers, drivers' license numbers, biometric information, and other information that could essentially be used for identity theft—were and are required to notify consumers in the event of a data breach.[6] A data breach is considered any event where data is accessed or acquired in an unlawful manner, and can range from malicious hacking to the simple loss of an unencrypted device holding the data.[7]

CCPA adds to existing breach-notification requirement by providing consumers with a private right of action in the event that the company that was breached did not employ "reasonable" data security measures.[8] Unfortunately, this term is not defined by the laws or CCPA's implementing regulations, leaving many companies guessing as to what exactly qualifies as a reasonable security measure.

A number of commentators, however, argue that the "reasonable" security measure requirement is actually extremely stringent and incorporates all 20 controls set forth in the Center for Internet Security's (CIS) Critical Security Controls (the Controls), citing a 2016 California Attorney General Report.[9] The Controls are separated into basic, foundational, and organizational security controls, and include security controls ranging from basic to sophisticated, and include security controls such as:

1. Inventorying and controlling hardware and software assets.
2. Continuous vulnerability management.
3. Controlled use of administrative privileges.
4. Secured configuration of hardware and software on mobile devices, laptops, workstations, and servers.
5. Email and web browser protection.
6. Malware defenses.
7. Secure configuration for network devices (e.g., firewalls, routers, and switches).
8. Incident response and management.
9. Penetration testing.[10]

Additionally, the Report indicates that the Controls are simply the "minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."[11]

Therefore, to the to the extent that the term "reasonable security procedures" is determined to mean implementation of the Controls, there are a number of key takeaways for any CCPA-regulated business:

1. Businesses will need to thoroughly examine the Controls to determine which Controls actually apply to their operations. For example, businesses that provide employees with laptops or other mobile devices will need to undertake more rigorous security compliance than those that do not.
2. Compliance will take a significant amount of time, effort, and most importantly, money. While some Controls may arguably be carried out by in-house personnel (especially for smaller enterprises), some tasks will inevitably require outside assistance. Without a technical staff, penetration

or securing network configurations may be impossible internally.
3. The Controls are a baseline, at least so long as the Report controls. Businesses that meet all 20 Controls may still be deemed to provide unreasonable security measures if their operations demand a higher level of security.

If a CCPA-regulated business is the victim of a data breach and did not have "reasonable security procedures" in place, a consumer can recover either actual damages, or statutory damages of between $100 and $750 per incident.[12] It is also important to note that while CCPA does not expressly allow the recovery of attorneys' fees, it does allow businesses to recover "[a]ny other relief the court deems proper,"[13] and this may be interpreted by courts to allow for the recovery of attorneys' fees that can be incredibly high in class-action litigation. Collectively, the potential of high damages could lead to financial ruin across the industry.

Licensed Cannabis Businesses and Personal Information

The State of California forces cannabis businesses to inspect, collect, and retain a vast amount of consumer personal information. As is examined in greater detail below, despite the vast amount of personal information cannabis companies are required to collect, the state imposes very few direct data security or protection requirements on such companies (instead, data protection requirements are found in other laws).

To understand why cannabis companies are required to collect so much information, a few points about the industry are critical to clarify. To start, California has programs for the sale of medical cannabis to qualifying persons. State law requires cannabis businesses to verify that persons have valid physicians' recommendations or medical marijuana identification cards (MMICs) in order to obtain medical-grade cannabis. Many cannabis businesses opt to store MMICs and recommendations.

MMICs and recommendations are deemed "medical information" and regulated under the California Confidentiality of Medical Information Act (CMIA).[14] They are therefore exempt from the CCPA, which carves out information regulated under certain

other federal and state laws.[15] That said, medical information is considered personal information for the purposes of California's breach notification statute.[16] It remains to be seen, however, whether CCPA's private right of action will extend to such breaches.

California also allows sales of recreational cannabis to persons over age 21. Cannabis businesses must verify that persons are at least 21 by reviewing driver licenses or other forms of government-issued identification. Driver license and certain other identification numbers are also deemed personal information for the purposes of California's breach notification statute.[17]

California also imposes extreme security requirements on cannabis businesses, many of which require cannabis companies to collect consumer personal information. For example, retail cannabis businesses are required to maintain security cameras that can allow for the recording of actual facial features of customers at the point of sale.[18] Facial images may be considered biometric data and fall within the confines of the California data breach statute.[19]

California cannabis laws also create unique pitfalls for cannabis companies. For example, the regulations expressly allow multiple licensees within one building to share video security systems and footage.[20] Given that footage may contain protected categories of information, this can invite violations of data security laws or the companies' own privacy policies. Cannabis companies that do share any kind of video surveillance data with their neighbors must be extremely vigilant in how they disclose data sharing in any kind of privacy policy.

Cannabis businesses must also be aware that they will be required to share virtually all collected information with government agencies. For example, cannabis delivery companies must provide delivery customers with receipts bearing their first name, address, and a specially assigned number (crafted using personal information that must be able to identify the consumer by more than just first name).[21] Licensees must therefore gather information concerning the name, age, physical location, and other qualities of delivery customers and maintain them in a way that allows the businesses to immediately identify customers to the state cannabis agencies on request. And for good measure, most such records must be maintained for seven years (the notable exceptions are video records, which must be maintained for only 90 days).[22]

To date, there are very limited requirements for what cannabis businesses must do with the data they collect, which is somewhat

surprising given that California regulates nearly all other aspects of cannabis businesses' operations. Instead, California cannabis businesses must look only to CCPA and other similar laws.

The notable exception was Assembly Bill 2402 (2018), which categorizes MMICs and physicians' recommendations as medical information and prohibits cannabis businesses from disclosing consumer personal information to third parties without consent (subject to certain exceptions). AB-2402 was fairly limited in scope, especially considering the breadth of information that cannabis businesses obtain. And because its requirements were not enshrined in California's cannabis regulations, many businesses remain unaware of them.

Non-Legal Personal Information Issues for Cannabis Businesses

In addition to the legal requirement to interact with and maintain personal information, there are a number of industry and other pressures that make cannabis businesses particularly susceptible to data breaches and CCPA litigation, and that can lead to severe unintended consequences.

First, cannabis businesses often collect much more personal information than they are legally required to, often to personalize users' experience, for marketing purposes, or just because they do not have rigorous data security programs in place. This raises the threat of additional damages and exposures in the event of data breaches.

Second, cannabis businesses are often underequipped and underprepared when it comes to cyber security. Obtaining state and local permits and licenses, paying ultra-high taxes with very limited federal deductions due to federal illegality, and operating a cannabis business are all extremely expensive, disincentivizing compliance with any law that is not specifically addressed to cannabis businesses. Spending tens of thousands of dollars implementing a state-of-the-art data security program is not in the cards for many cannabis companies, and hackers will eventually figure that out.

Third, despite the fact that more than 30 states and the District of Columbia now have some form of cannabis decriminalization or legalization, cannabis (even for medical use) remains illegal pursuant to the federal Controlled Substances Act and cannabis

remains a Schedule I controlled substance thereunder.[23] Cannabis also remains illegal in a handful of states. Cannabis companies that are the victims of data breaches may be required to provide notice to state attorneys general or federal regulators, or may wish to report certain incidents to federal agencies. These kinds of incidents can draw unwanted scrutiny and treatment from state and federal agencies and lead to a host of unintended consequences.

Fourth, reputational harms can destroy cannabis businesses. In states like California with growing cannabis industries, virtually all businesses are start-ups with limited operating history and a desperate need for capital given the extreme costs identified above. Data breaches not only have the potential to lead to massive lawsuits, discussed in greater detail below, but also have the potential to end investment capital, which could mean the life of a business.

Finally, data breaches can be devastating even apart from CCPA litigation because they can interrupt revenue streams. If a data breach results in licensees' loss of connectivity to the state-mandated track-and-trace program (which tracks cannabis from seed to sale), licensees may not "transport, receive, or deliver any cannabis goods until such time as connectivity is restored."[24] In the event of a ransomware attack that limits access to the track-and-trace system, businesses may literally be unable to operate for days or even weeks.

In sum, in addition to the vast amounts of information that cannabis businesses are required to store or store by choice, reputational harm, unwanted government scrutiny, and debilitating regulatory conditions can lead to serious financial woes for cannabis businesses. On top of all of those problems, if a company did not maintain what the state deems to be a "reasonable" security program, that company could face bet-the-company class action litigation. Below is an example of how severe data breaches can be for regulated cannabis businesses.

Case Study in CCPA Damages

ABC Co. is a licensed cannabis dispensary in a major California city. To personalize customers' shopping experience and speed up future purchases, ABC's budtenders gather copies of the consumer's government-issued ID, combined with consumer information such as first and last name, address, phone number, email, and date of

birth. All of ABC's employees have access to the system using one, generic password. The company did not have any formal data security program. ABC does not have any kind of insurance in place that would insulate it from damages in the event of a data breach or litigation alleging claims under CCPA.

An ABC employee was the victim of a phishing scam. The ABC employee had the password to the customer profile program in the employee's email. During a subsequent investigation, investigators determine that the program was accessed by a non-employee. ABC determines that more than 3,000 California consumers' information was accessed by the hacker and provides notice to each California consumer in accordance with California's breach notification statute.

ABC is sued by a class of 3,000 consumers seeking statutory damages. The complaint alleges that the company had no security program in place and that it was reckless to share the one company-wide password via email. The complaint also cites to a previous data breach pre-dating CCPA and the company's failure to undertake any remedial measures. The class seeks damages of $750 per consumer, for a total of $2,250,000.

Alternatively, some consumers opt to sue individually, alleging that they were harmed by the data breach and seeking actual damages exceeding $750 each. One consumer alleges that she was the victim of identity theft and lost several thousand dollars. Another consumer was a federal employee and lost his job as a result of the data breach and the discovery of that employee's cannabis use.

It is not difficult to foresee how cases like this could proceed in the future. Companies like ABC that do not maintain sufficient levels of insurance and do not have millions of dollars available to settle disputes of this magnitude can face tremendous liability if they fail to comply with CCPA.

What Cannabis Companies Can Do

The deck is stacked against many companies in the cannabis industry and the cannabis regulations provide very little guidance as to how companies can operate securely. There are a few considerations for any cannabis business that can mitigate against the risks posed by CCPA.

First, companies must make themselves aware of and comply with all relevant privacy laws. Many cannabis companies have

myopic views of the regulations, focusing only on those specific sets of regulations that apply directly to their operations. This is a huge mistake. Cannabis companies need to evaluate whether CCPA applies to their enterprise, and if it does, figure out how to comply. There is no shortage of plaintiffs' attorneys in California, and well-funded, non-compliant cannabis businesses will make easy targets.

Second, companies should target the Controls or other information security standards. While it is not yet clear what exactly is "reasonable" in terms of security, it is apparent that companies that employ rigorous security programs and make efforts to meet accepted security standards will be less likely to be in the crosshairs of class action litigants. Secured businesses, after all, are less likely to be sued in the first place.

Third, cannabis companies should prepare for data breaches or other data security incidents. Training employees, and having plans for what to do in the event of a breach, could also avoid or lessen the impact of a breach or the potential class of consumers whose information is affected. For example, if a company is able to cut off access to an affected system within five minutes of being alerted to a potential breach due to rigorous employee training, that company may substantially mitigate consumer harm and potential damage.

Fourth, cannabis companies should consider comprehensive insurance policies. Shockingly, state-level insurance requirements for cannabis businesses are sparse, and only cannabis distributors (business-to-business licensees that do not interact with consumers and generally obtain much less personal information) are specifically required to obtain commercial general liability insurance.[25] Cannabis companies should seriously consider all forms of insurance that would mitigate against data security incidents as well as potential legal actions that are fallouts of data security incidents.

The more prepared any company is, the lesser the chance that it will be victimized or face severe damages if it is victimized. Because the stakes are so much higher for cannabis companies than for many other companies, preparation should not be delayed or avoided.

Notes

* Griffen Thorne (griffen@harrisbricken.com) is an attorney in the Los Angeles office of Harris Bricken, an international emerging markets law firm. With both litigation and transactional experience, he represents clients in a

number of emerging fields, including in the cannabis and hemp industries and involving complex regulatory and data security matters.

1. Cal. Assembly Bill 375 (2018). For some of the amendments, see Assembly Bills 25 (2019), 874 (2019), 1146 (2019), 1355 (2019), and 1564 (2019).
2. Cal. Civ. Code § 1798.198(a).
3. *Id.* § 1798.105(a).
4. *E.g.*, Cal. Civ. Code § 1798.130(a)(5).
5. *See* 11 C.C.R. § 999.308 (describing requirements for privacy policies).
6. *See* Cal. Civ. Code §§ 1798.81.5(d) (defining "personal information"), 1798.82 (identifying breach notification requirements).
7. *Id.* § 1798.82(g).
8. *Id.* § 1798.150(a)(1).
9. *See* Joseph J. Lazzarotti & Jason C. Gavejian, *CCPA Data Breach Class Action Litigation Begins*, Nat'l Law Rev. (Feb. 6, 2020), https://www.natlawreview.com/article/ccpa-data-breach-class-action-litigation-begins (citing California Data Breach Report, Cal. Att'y Gen. (Feb. 2016), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (the "Report")); Jaime B. Petenko, *The California Consumer Privacy Act and "Reasonable Security": A Game Changer*, McDermott Will & Emery (Jan. 9, 2020), https://www.mwe.com/insights/the-california-consumer-privacy-act-and-reasonable-security-a-game-changer/ (citing the Report); *see also* Bryan Cave Leighton Paisner, *What Are "Reasonable Security Procedures and Practices" Under the CCPA?*, https://ccpa-info.com/what-are-reasonable-security-procedures-and-practices-under-the-ccpa/ (last visited Sept. 7, 2020) (citing the Report).
10. *See The 20 CIS Controls & Resources*, Ctr. for Internet Security, https://www.cisecurity.org/controls/cis-controls-list/ (last visited Sept. 7, 2020).
11. Report at v.
12. Cal. Civ. Code § 1798.150(a)(1)(A).
13. *Id.* § 1798.150(a)(1)(C).
14. Cal. Bus. & Prof. Code § 26162.5.
15. Cal. Civ. Code § 1798.145(c)(1)(A).
16. *Id.* § 1798.82(h)(1)(D).
17. *Id.* § 1798.82(h)(1)(B).
18. 16 C.C.R. § 5044(e).
19. Cal. Civ. Code § 1798.82(h)(1)(F).
20. 16 C.C.R. § 5044(*l*).
21. *Id.* § 5420.
22. *Id.* §§ 5037, 5044(h).
23. 21 U.S.C. § 841(a); *id.* § 812(c), Sched. I § (c)(10).
24. 16 C.C.R. § 5050(b).
25. 16 C.C.R. § 5308.