



CANNABIS COMPANIES

Don't Overlook Data-Related Litigation Risks

BY BARAK COHEN, DAVID BIDERMAN, AND TOMMY TOBIN

Cannabis business faces a dizzying array of federal and state laws presenting significant challenges for companies attempting to comply with this increasingly complex patchwork of rules. As the cannabis industry continues to grow in both sales and sophistication, an increasing number of jurisdictions have now adopted rules for the medical and recreational use of marijuana.¹ After the November 2020 election, medical marijuana is legal in over thirty-five jurisdictions, and recreational uses are permitted in fifteen states and the District of Columbia. In fact, the number of states in which cannabis is being legalized grows so rapidly that it is difficult to track these numbers from week to week. Unfortunately, the growth of the cannabis industry has increasingly made these companies targets for data-related litigation, especially for private enforcement of California's data privacy laws and the Telephone Consumer Protection Act (TCPA).

A CHANGING PRIVACY LANDSCAPE AT THE FEDERAL AND STATE LEVELS

In the United States, federal and state governments are increasingly focused on consumer privacy and the regulation of consumer data. For example, at the federal level, Congress enacted the TCPA in 1991 to govern the use of automatic telephone dialing systems to send unwanted phone, text, and fax messages.² Pursuant to the statute, the Federal Communication Commission (FCC) has issued regulations outlining specific compliance obligations.³ The law has been interpreted in recent years to cover a broad array of automated dialing systems, including many systems that help businesses reach out to their customers by phone and text.⁴ The statute provides for penalties of \$500 to \$1,500 per violation, meaning that even a modest amount of unsolicited messages can create significant exposure. One unsolicited message, for example, sent to 1,000 recipients could lead to exposure of \$500,000 to \$1.5 million.

Even though the TCPA is now turning thirty years old, it continues to be relevant today. Between 2010 and 2017,

the number of TCPA litigation matters has increased dramatically, with sources claiming the number has grown by more than 1,200 percent.⁵

Given that the statutory damages available to litigants under the TCPA are uncapped, the TCPA is naturally favored by the plaintiffs' bar. Recent months have seen plaintiffs targeting cannabis companies in particular, with more than a dozen class action matters already filed across the country, including cases in Arizona, California, Florida, Michigan, and Nevada. More are filed every week.

On the state level, California is of particular importance for its leadership within the United States regarding data privacy laws.⁶ Passed in 2018, the California Consumer Privacy Act (CCPA) is the nation's most sweeping data privacy law. The law went into effect in January 2020 and created new obligations for businesses in collecting and maintaining data related to California consumers. The CCPA created a set of consumer data privacy rights for California consumers, including, but not limited to, a right to know about the collection of personal information, the right to opt out of particular sales of that personal information, the right to access such information, and the right not to be discriminated against by a company for asserting the consumer's privacy rights. The CCPA's definition of protected information is expansive, including usernames and passwords, biometric data, and account numbers.

To enforce these new consumer rights and corresponding business obligations, the law provides for two enforcement options: the state attorney general and California consumers themselves, to whom the law grants a limited right of action. The precise scope of this private right of action is yet to be borne out as the law has only recently come into effect.

When asked about how his office would enforce the CCPA, California Attorney General Xavier Becerra stated that California's top law enforcement officials would look kindly on businesses that demonstrated "an effort to comply" but "descend" on those that were not

operating properly "to make an example of them."⁷ Enforcement of the CCPA began in July 2020, with its final regulations issued in August 2020.⁸ The state attorney general wasted no time, sending out initial warning letters the day that enforcement began in July 2020.⁹ Since then, Attorney General Becerra's office has announced at least two multimillion-dollar settlements regarding data breaches, including against a health insurance company and a mobile app allegedly failing to maintain adequate data security measures.¹⁰

With respect to private rights of action under the CCPA, the law permits California consumers to file suit when a business violates its duties to "implement and maintain *reasonable security procedures and practices*," leading to the "unauthorized access and exfiltration, theft, or disclosure" of "nonencrypted and nonredacted personal information" of those consumers.¹¹ The law does not define what constitutes "reasonable security procedures and practices." Damages for violating the CCPA are set at between \$100 and \$750 per consumer, per violation, in addition to injunctive or declaratory relief and "any other relief the court deems proper."¹² The extent of these damages turns on the "nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."¹³ The contours of the CCPA's private right of action are continuing to take shape in recent months as litigants file an increasing number of lawsuits referencing the CCPA.¹⁴ Over 100 class action matters have already been filed referencing the CCPA since January 2020, and further CCPA litigation "seems likely, as litigants seek to define the scope of this remedy for consumers."¹⁵

In November 2020, California voters again led the country in approving even more robust privacy protocols, this time by passing the California Privacy Rights Act (CPRA). The CPRA expands upon the CCPA's framework, including the CCPA's private right of action, allowing

suits when a consumer's email and password are breached.¹⁶ In addition, the CPRA creates a new state agency for enforcement and regulation regarding consumer data. The CPRA is slated to go into effect in 2023 and will layer on new obligations for businesses handling data relating to California consumers, including cannabis companies.

TCPA AND CCPA SUITS INCREASINGLY TARGET CANNABIS COMPANIES

From dispensaries to manufacturers, cannabis companies are at increased risk of TCPA and CCPA suits.

At least one cannabis company has already been targeted by a class action alleging violation of state privacy laws, including the CCPA.¹⁷ The cannabis industry might see further class action litigation alleging CCPA violations for several reasons. First, California is a significant market for cannabis products, whether it be THC (the psychoactive substance most associated with a marijuana "high") or hemp-derived cannabidiol (CBD). Second, the sensitive data held by cannabis companies, particularly those in the medical marijuana space, make them a target for potential data loss.¹⁸ Third, as nascent ventures, many cannabis companies may be relatively unsophisticated regarding data protection and data privacy protocols compared to larger companies in more mature industries.

With respect to the TCPA, in April 2019, a cannabis company settled a TCPA suit for \$1.75 million involving over 50,000 customers.¹⁹ In March 2020, TCPA allegations were brought against a dispensary company along with a demand of \$500 per unwanted text.²⁰

As TCPA allegations continue to target cannabis companies, at least one cannabis delivery service has defeated class certification.²¹ For example, in *Derval v. Xaler*, the Central District of California found that putative class plaintiffs had initially proposed thousands of class members but ultimately provided no "support that any of those customers received unwanted text messages, revoked consent to receive messages, or continued to receive messages after revocation."²²

FROM DISPENSARIES TO MANUFACTURERS, CANNABIS COMPANIES ARE AT INCREASED RISK OF TCPA AND CCPA SUITS.

TCPA litigation facing the cannabis industry shows no signs of abating, and companies should take steps to mitigate the risks posed by the law. Such steps include, but are not limited to, training marketing and advertising employees about the TCPA and developing systems to recognize and honor opt-out requests.²³

WHAT DOES THIS MEAN FOR CANNABIS COMPANIES?

Cannabis companies, particularly those in the medical marijuana industry, often have access to sensitive information about their consumers. For marijuana companies, many state laws require the company to collect and maintain such information, including photo identification and health records. Unfortunately, this can make these companies targets of data losses.²⁴ Given the fact that these companies are targets for potential data loss, the failure to take reasonable measures to secure personal information can create considerable legal risk, particularly for marijuana companies.²⁵

Because cannabis companies are sometimes required to collect sensitive information, such as photo identification or date of birth, to comply with state laws, data breaches of these companies can expose personal information for customers. For example, researchers in January 2020 found a data breach that had exposed the full names, phone numbers, dates of births, medical ID numbers, signatures, gram limits, and sales figures of 30,000 medical marijuana customers.²⁶

The risks of data breaches are especially elevated for medical marijuana companies, as these companies might collect and possess data subject to the federal Health Insurance Portability and Accountability Act (HIPAA) as well as state laws. The sanctions for HIPAA violations can be severe, including the imposition of possible civil and criminal penalties.

Given the risks of data breaches and the sensitive information to which many businesses in the marijuana industry are privy, taking proactive steps to mitigate the risks of data loss can be helpful. Such steps include establishing data privacy and data security policies and refreshing them as needed, implementing and maintaining reasonable security measures to safeguard consumer and employee information, and training employees in cybersecurity and the avoidance of social engineering attacks, such as phishing.²⁷

CONCLUSION

The growth of the cannabis industry has created new opportunities for businesses to expand their sales and reach new consumers, especially as new jurisdictions adopt legalized marijuana programs. Amid this growth comes considerable regulatory ambiguity, as cannabis businesses attempt to comply with myriad state and federal regulations regarding cannabis. Within this patchwork of complex federal and state (and even local) rules regarding the operation of legal cannabis companies, the industry cannot overlook data-related litigation

risks, especially compliance with new privacy laws affecting California consumers, and mitigating the risks posed by a recent wave of TCPA suits targeting cannabis companies.

Barak Cohen is chair of the Perkins Coie LLP's Cannabis Industry Group, which he helped establish; a partner in the firm's White Collar & Investigations practice; and lead for commercial litigation in the firm's Washington, D.C., office. He also edited and co-authored the ABA treatise Cannabis Law: A Primer on Federal and State Law Regarding Marijuana, Hemp, and CBD. David Biderman, a partner in Perkins Coie's San Francisco and Los Angeles offices, focuses his practice on mass tort litigation and consumer class actions. He heads the firm's Consumer Products & Services Litigation group. Tommy Tobin, an associate in Perkins Coie's Seattle office, focuses on complex commercial litigation and class action matters involving statutory, constitutional, and regulatory issues in a range of industries, including food and beverage, consumer packaged goods, and cannabis. He is a member of the Editorial Board of The SciTech Lawyer.

ENDNOTES

1. See Barak Cohen, Jason Howell & Tommy Tobin, *Considerations for Marketing Cannabis Amid Varied Laws*, LAW360 (Nov. 30, 2020), <https://www.law360.com/articles/1331801>.

2. See 47 U.S.C. § 227.

3. See 47 C.F.R. § 64.1200 et seq.

4. David Biderman, Barak Cohen, Nicola Menaldo & Tommy Tobin, *Cannabis Businesses Should Get Smart About TCPA Litigation Risks* (July 6, 2020), <https://news.bloomberglaw.com/us-law-week/insight-cannabis-businesses-should-get-smart-about-tcpa-litigation-risks>.

5. *TCPA Litigation Continues to Skyrocket; 1,272 Percent Increase Since 2010*, U.S. CHAMBER OF COM., INST. FOR LEGAL REFORM (Jan. 27, 2017), <https://instituteforlegalreform.com/tcpa-litigation-continues-to-skyrocket-1272-percent-increase-since-2010/>; see also *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, U.S. CHAMBER OF COM., INST. FOR

LEGAL REFORM (Aug. 31, 2017), <https://instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits/> (“federal court dockets are overburdened with TCPA litigation”).

6. See Dominique Shelton-Leipzig, David Biderman, Chris J. Hoofnagle & Tommy Tobin, *Can California's Privacy Initiative Revitalize U.S.-EU Commerce?* 7 PRATT'S PRIV. & CYBERSECURITY L. REP. 15 (2021).

7. Nandita Bose, *California AG Says Privacy Law Enforcement to Be Guided by Willingness to Comply*, REUTERS (Dec. 10, 2019), <https://www.reuters.com/article/us-usa-privacy-california/california-ag-says-privacy-law-enforcement-to-be-guided-by-willingness-to-comply-idUSKBN1YE2C4>.

8. See Marina Gatto & Dominique Shelton-Leipzig, *The Final California Consumer Privacy Act Regulations Are in Effect*, PRIV. QUICK TIPS (Aug. 18, 2020) <https://www.privacyquicktipsblog.com/2020/08/the-final-california-consumer-privacy-act-regulations>.

9. Allison Schiff, *It May Seem All Quiet on the CCPA Front, but Don't Get Complacent: CCPA Enforcement Has Begun*, ADXCHANGER (Sept. 28, 2020), <https://www.adexchanger.com/privacy/it-may-seem-all-quiet-on-the-ccpa-front-but-dont-get-complacent-ccpa-enforcement-has-begun>.

10. *Privacy Enforcement Actions*, CAL. ATT'Y GEN., <https://oag.ca.gov/privacy/privacy-enforcement-actions>.

11. CAL. CIV. CODE § 1798.150(a)(1) (emphasis added).

12. *Id.* § 1798.150(c).

13. *Id.* § 1798.150(a)(2).

14. See Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, IAPP NEWS (June 8, 2020), <https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action>.

15. *Id.*; see also Megan Gates, *CCPA Deep Dive: How California Is Enforcing Its Major Privacy Law*, SEC. MGMT. (Dec. 1, 2020), <https://www.asisonline.org/security-management-magazine/articles/2020/12/ccpa-deep-dive-how-california-is-enforcing-its-major-privacy-law/>; *CCPA Litigation Year in Review*, PERKINS COIE

(Mar. 2021), <https://www.perkinscoie.com/en/ccpa-litigation-tracker.html>.

16. See OneTrust, *CCPA v. CPRA—What Has Changed?*, ONE TRUST BLOG (Nov. 10, 2020), <https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/>.

17. See *Warshawsky v. cbdMD, Inc.*, No. 3:20-cv-00562-RJC-DSC (W.D.N.C. filed Oct. 9, 2020).

18. See Barak Cohen, Amelia Gerlicher, Charlyn Ho & Tommy Tobin, *Mitigating Data Breach Risks Facing Marijuana Businesses*, BLOOMBERG LAW (July 27, 2020), <https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-mitigating-data-breach-risks-facing-marijuana-businesses>.

19. Allison Grande, *Calif. Marijuana App to Shell out \$1.75M to End TCPA Suit*, LAW360 (Apr. 2, 2019).

20. Jack Queen, *Weed Dispensary Hit with TCPA Suit Alleging Spam Text*, LAW360 (Mar. 31, 2020).

21. *Derval v. Xaler*, No. 2:19-cv-01881-ODW (C.D. Cal. Jan. 28, 2020), Dkt. 38.

22. *Id.* at *5.

23. David Biderman, Barak Cohen, Nicola Menaldo & Tommy Tobin, *Cannabis Businesses Should Get Smart About TCPA Litigation Risks*, BLOOMBERG LAW (July 6, 2020), <https://news.bloomberglaw.com/us-law-week/insight-cannabis-businesses-should-get-smart-about-tcpa-litigation-risks>

24. Cohen et al., *Mitigating Data Breach Risks*, *supra* note 18.

25. *Id.*

26. Jason Murdock, *Data Breach Exposes Personal Details of Over 30,000 U.S. Cannabis Users*, NEWSWEEK (Jan. 23, 2020).

27. Cohen et al., *Mitigating Data Breach Risks*, *supra* note 18.