Articles in the Journal of Equipment Lease Financing are intended to offer responsible, timely, in-depth analysis of market segments, finance sourcing, marketing and sales opportunities, liability management, tax laws regulatory issues, and current research in the field. Controversy is not shunned. If you have something important to say and would like to be published in the industry's most valuable educational journal, call 202.238.3400.

The Equipment Leasing & Finance Foundation
1625 Eye St NW,
Suite 850
Washington, DC 20006
202.238.3400
www.leasefoundation.org

EDITORIAL BOARD

EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

CONNECT WITH THE FOUNDATION

JOURNAL

OF EQUIPMENT LEASE FINANCING

VOLUME 37 • NUMBER 3 • FALL 2019

Commercial Lenders Brace for Consumer-Style Disclosures in California and Beyond

By Clinton R. Rockwell, Kathryn L. Ryan, Moorari K. Shah and Frida Alim

One year ago, California became the first state to require consumer-style disclosures similar to those required for consumer loans under federal laws. The requirements of Senate Bill 1235 signal a sea change likely to affect other states as well. This article, the first of two, explains the implications for the equipment leasing and finance industry.

Privacy Puzzle — Grappling with the Patchwork of New State-Specific Data Privacy Laws

By Andrew Baer and Matthew Klahre

Lessors conducting business in California must pay attention to the evolving and sometimes puzzling amendments to the California Consumer Protection Act. The act affects both business-to-business and business-to-consumer transactions. Several other states also are enacting laws that signify compliance challenges for national and international businesses.

Blockchain: Transforming Public Data for Improved Financial Success

By Raja Sengupta

Blockchain has the potential to help states establish and demonstrate transparency, speed up processing times, and cut operational costs related to commercial lending. That augers well for states vying to attract new businesses. Advances such as "smart UCCs" will benefit lenders, too. Where they can conduct due diligence easily, they will be more apt to do business.

Copyright © 2019 by the Equipment Leasing & Finance Foundation • ISSN 0740-008X

Privacy Puzzle: Grappling With the Patchwork of New State-Specific Data Privacy Laws

By Andrew Baer and Matthew Klahre

Lessors conducting business in California must pay attention to the evolving and sometimes puzzling amendments to the California Consumer Protection Act. The act affects both business-to-business and business-to-consumer transactions. Several other states also are enacting laws that signify compliance challenges for national and international businesses.

From a privacy compliance perspective, operating a global business has never been more complicated. Just as businesses and privacy practitioners have come to grips with the General Data Protection Regulation (GDPR)[1] (the European Union's unprecedented, extraterritorial privacy regime with eye-watering penalties for noncompliance[2] that became effective May 25, 2018), businesses with operations in the United States are now confronted with another privacy compliance challenge: a patchwork of several new state-specific privacy laws, each with its own unique set of operational and legal requirements (and penalties).

The most controversial of these new U.S. state privacy laws is the California Consumer Protection Act (CCPA), which has been coined "California's GDPR," given its sweeping scope, unprecedented degree of protection of covered data subjects, and puzzling text.

Despite the use of "consumer" in its title and throughout its text, the CCPA will apply to information relating to all individuals, regardless of whether it is processed in the business-to-business or business-to-consumer context. As such, CCPA compliance will be important for any organization that is doing business in California, even if it does not interact with traditional "consumers."

Other states, such as Nevada and Massachusetts, have also proposed or enacted new privacy laws of their own. Each state's law is different, which means that operationalizing compliance with the most stringent of these new state regimes does not guarantee compliance across the board, nor does compliance with the GDPR ensure compliance with these state-specific U.S. regimes.

This article will provide a high-level overview of some of these new state laws with a particular emphasis on the CCPA, and it will offer answers to some of the pressing questions that businesses of all sizes should be asking as these new laws come into effect.

CALIFORNIA CONSUMER PROTECTION ACT

Background

The CCPA was enacted in June of 2018 and is expected to become effective on January 1, 2020. However, due to the unusual circumstances surrounding its inception, the effective date – and the law itself – are still subject to change.

Only a few days after the CCPA was conceived as a ballot initiative sponsored by a real estate investor, the California legislature introduced its own version of the bill, as a compromise to prevent the original initiative from making it to the polls (since passage as a ballot initiative would have made future amendments to the law extremely difficult to enact). As a result of its swift drafting, the bill had to be amended only two months later. Indeed, the many glaring errors and inconsistencies that still remain in its current text suggest that more changes are coming.

Additionally, as of the date of this writing, the California attorney general has yet to act on the CCPA's mandate to promulgate rules and guidance expanding and clarifying the scope of the law, which are now expected to be issued

The expansive definition of what is considered to be "personal information" for CCPA purposes is one of the most controversial and unprecedented portions of the law.

by fall 2019, and which many hope will shed some light on how to overcome the practical challenges that its implementation will raise.

Regardless of the many contradictions and voids in its current drafting, businesses that will be subject to the CCPA should begin to implement data privacy policies and procedures that enable them to be compliant with their newly created obligations in time for January 1, 2020.

Businesses Subject to the CCPA

The CCPA will apply only to those for-profit entities that:

(a) collect (including buying, renting, gathering, obtaining, receiving, or accessing by any means) "personal information" from "consumers" (each defined below), or on behalf of which such information is collected,

(b) alone or jointly with others determine the purposes and means of processing such personal information,

(c) do business in California, and

(d) either (1) have $25 million or more in annual revenues, (2) derive 50% or more of their revenues from selling (which includes disclosing in exchange for any consideration) personal information, or (3) annually buy, receive, sell, or share personal information from 50,000+ California consumers.[3]

The law also applies to corporate affiliates that share common branding with a covered business,[4] but it does not apply in certain circumstances, such as if every aspect of the commercial conduct occurs entirely outside of California,[5] if the information is collected to complete a single, one-time transaction,[6] or if personal information is being sold as part of a merger or acquisition deal.[7]

The CCPA defines "consumers" as natural persons who are California residents for tax purposes, and therefore includes both individuals who are in the state for other than temporary purposes as well as those individuals who are domiciled in California but are out-of-state for a temporary purpose.[8] Notably, despite the restrictive meaning that is usually associated with the term "consumer," for purposes of the CCPA, a "consumer" is also an individual contact in a business-to-business relationship.

The expansive definition of what is considered to be "personal information" for CCPA purposes is one of the most controversial and unprecedented portions of the law: it includes not only traditionally-protected personally identifying information of consumers, but also information "capable of being associated with, or [which] could reasonably be linked, directly or indirectly, with a particular consumer or household."[9]

(California Assembly Bill 874, if signed by Governor Gavin Newsom, would clarify that information must be "reasonably" capable of making the foregoing associations or links in order to qualify as personal information under the CCPA,[10] which some advocates suggest will make this otherwise sweeping definition more workable.)

The CCPA gives some non-exhaustive examples of what categories of personal information are included in this definition, which includes traditionally personally identifiable information, such as one's internet protocol (IP) address, unique personal identifiers, and online identifiers.[11]

Also included are broad categories such as "purchasing or consumer histories and tendencies," biometric and geolocation data, "internet or other electronic network activity information," "audio, electronic, visual, thermal, olfactory, or similar information," and even more interestingly, "inferences drawn from any of the [categories of personal information listed] to create a profile about a consumer."[12]

Further, the current iteration of the CCPA does not exclude employee data from "personal information"; however, California A.B. 25, if signed by the governor, would narrow the definition of "consumer" to exclude job applicants, employees, agents, and contractors until January 1, 2021, thereby temporarily relieving employers of certain CCPA obligations with respect to the data of their own personnel.[13]

However, even during this one-year moratorium, these individuals would still have the right to be informed of the categories of personal information collected by their employers and the purposes for which it was used, and the right to bring a private right of action against their employer for a data breach.[14]

Similarly, California A.B. 1355, if signed by the governor, would exempt until January 1, 2021, certain business contact information that a business collects during communications or transactions with another business.[15]

The current definition of personal information does not clearly include de-identified or aggregate consumer information or information that is publicly available from government records,[16] and clear exclusions of this information from the definition of personal information would be cemented by Califor-

nia A.B. 874, if signed by the governor.[17]

It is important to note that the law applies not only to information collected online or electronically but also through other methods, such as in person or through the use of an algorithm. The breadth of this definition means that conducting data inventories and mapping will be a challenge for businesses subject to the new law, highlighting the importance of implementing compliance efforts as far in advance as possible.

Consumer Rights Under the CCPA

The newly created rights for consumers protected by the CCPA include:

- the right to know what personal information a business collects, sells, and discloses about consumers generally, and about a particular consumer as well;
- the right to request access to a copy of the specific pieces of personal information that the business has collected about them;
- the right to request that the business does not sell their personal information;
- the right to request that the business delete (and direct its service providers to delete) all personal information collected about them (subject to certain exceptions); and
- the right to be free from discrimination in the event they choose to exercise any of these rights.[18]

The covered business must, within 45 days from its receipt of a consumer's verified request:

- disclose the categories and specific pieces of the consumer's personal information that the covered business has collected during the 12-month period preceding the request,
- the categories of sources from which the personal information was collected,
- the business or commercial purposes for collecting or selling the personal information, and
- the categories of third parties with whom the business shares personal information.[19]

With respect to consumers' rights to opt out of the sale of their personal information in particular, a covered business will need to implement on its website a clear and conspicuous Do Not Sell My Personal Information link to effectuate such opt-outs.[20]

In addition, if a covered business shares California consumers' personal information with its service providers or with unaffiliated third parties, it is also prudent for the covered business to revise its written agreements with its service providers and third-party recipients of data to include the CCPA's recommended downstream data retention, use, and disclosure restrictions.[21]

While these downstream restrictions are not mandatory under the CCPA, including them will allow a covered business to limit its liability for penalties under the CCPA in the event of a violation by a service provider or third party.

Penalties Under the CCPA

If a covered business fails to comply with the CCPA, the California attorney general will have the power to bring civil actions.[22] If a business fails to cure an alleged violation within 30 days of being notified of noncompliance, penalties can be imposed of up to $2,500 per unintentional violation, and up to $7,500 per intentional violation.[23]

Additionally, private plaintiffs will be able to institute civil actions for the unauthorized access, theft, or disclosure of non-encrypted or nonredacted personal information due to the business's failure to implement reasonable security practices and procedures, with the caveat that the definition of personal information in this context includes only a consumer's first name or initial and last name in combination with their

- Social Security number,
- driver's license number (or California ID card number),
- account name, credit card, or debit card number, in combination with a code that would give access to a financial account,
- medical information, or
- health insurance information.[24]

Potential damages in actions brought by consumers include statutory damages ranging from $100 to $750 per consumer per incident or actual damages (whichever is greater), injunctive or declaratory relief, or any other relief the court deems proper.[25] Statutory damages will be available only if the consumer provided the business with 30 days' written notice prior to filing the data-breach lawsuit.[26]

If the violation can be cured and the business actually cures the noticed violation and provides the consumer with a written statement that the violation has been cured and no further violations will occur, then statutory damages will not be available.[27] However, if the business violates the written statement, the consumer may then sue to enforce the statement and recover statutory damages for each breach of the written statement as well as for "any other violation of the [CCPA] that postdates the written statement."[28]

While these downstream restrictions are not mandatory under the CCPA, including them will allow a covered business to limit its liability for penalties under the CCPA.

If a business is subject to the CCPA, it will need to decide whether to extend CCPA rights to individuals residing outside of California.

GDPR Compliance Is Not Enough

Unfortunately, given some important differences between the GDPR and the CCPA, GDPR compliance will not guarantee that a business will be CCPA compliant. But businesses having GDPR policies and procedures in place will have a significant head start in their CCPA compliance efforts.

Some of the key differences between the two frameworks include:

- their scope and territorial reach (although both laws extend beyond the physical borders of their jurisdictions, the GDPR's reach is broader),
- the methods for obtaining consumer consent to the processing of their personal information (the GDPR requires affirmative opt-in consent, while the CCPA has an absolute right to opt out of the sale of personal information, as discussed above),
- the rights granted to consumers (although some of the rights overlap, the GDPR also affords consumers the right to correct or complete their personal information, the right to restrict its processing, and the right to object to its processing in some instances),
- the GDPR's requirement that companies establish a legal basis for processing personal information (which is not duplicated under the CCPA),
- the level of disclosures required (although similar, the information required and delivery methods differ),
- the definition of personal information (the CCPA's is broader),
- data-breach notification requirements,
- children's privacy rights, and
- potential liabilities.

Table 1 provides a direct summary and comparison of some of these key distinctions.

These differences will likely mean that the control processes designed by businesses for GDPR compliance will not be fit to ensure CCPA compliance without being amended, and that commercial agreements which have been amended for GDPR compliance will need further revision.

Additionally, if a business is subject to the CCPA, it will need to decide whether to extend CCPA rights to individuals residing outside of California, or, if on the other hand, it will handle personal information from California consumers separately from that of other individuals.

This assessment should take into consideration factors such as these three:

- whether the covered business is prepared to distinguish between the information collected from individuals residing in California and elsewhere,
- whether the covered business feels comfortable with allowing non-California data subjects to know that the business's California consumers have "more rights" with respect to their data privacy than they do, and
- whether it would make more economic sense to extend these rights to individuals from across the country, given that other states are in the process of adopting similar regulations, as discussed further below.

NEVADA AND MASSACHUSETTS

As mentioned above, California is just one of several states that have proposed or enacted new privacy legislation, and each law has a different focus. Nevada's law, Senate Bill 220, goes into effect on October 1, 2019, and focuses on Nevada consumers' online privacy.[29]

S.B. 220 is an expansion of Nevada's existing online privacy law, which requires covered operators of websites and online services to post a privacy policy disclosing their practices surrounding the collection and use of Nevada consumers' covered information.[30]

After S.B. 220 becomes effective, Nevada consumers must additionally be provided with a mechanism to opt out of the "sale" of covered information that the operator collects about them, and consumers must also be provided with a set of required disclosures to Nevada residents (which are different from those required under the CCPA and the GDPR).

As additional points of comparison, under the Nevada law a "sale" is narrowly defined as "the exchange of covered information for monetary consideration," and the definitions of "personal information" and "consumer" are different from those in the CCPA and the GDPR.

The Commonwealth of Massachusetts' privacy legislation, An Act Relative to Consumer Data Privacy, parallels many aspects of the CCPA, but with a broader definition of the information protected by the proposed law, and a lower revenue threshold for determining whether a business is subject to the act.[31]

The act also provides a private right of action and $750 in statutory damages per violation, with no cap on damages or the requirement that the data subject prove that he or she was actually harmed by the violation.

As of the date of this writing, the bill is under consideration by the

Table 1. Distinctions Between CCPA and GDPR Requirements

Data subject rights	CCPA	GDPR
Opt-out rights	A covered business must enable Californians to opt out of the sale of their personal information to third parties, and must include a Do Not Sell My Personal Information link in a clear and conspicuous location of the covered business's website homepage. A covered business must not request reauthorization to sell a consumer's personal information for at least 12 months after the consumer's opt out.	Requires affirmative opt-in consent, or the establishment of another lawful basis for processing. No specific right to opt out of sales of personal data. Data subjects can opt out of processing data for marketing purposes and withdraw consent for other processing activities.
Rights of rectification (correction)	None.	Data subjects have the right to correct and complete inaccurate personal data.
Right to restrict processing	None, other than the right to opt out from sales of personal information.	Right to restrict processing of personal data in circumstances.
Right to object to processing	None, other than the right to opt out from sales of personal information.	Right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes.
Right to object to automated decisionmaking	None.	Data subjects have the right not to be subject to automated decisionmaking based on their personal data (e.g., profiling).
Right of erasure/deletion	Consumers may request deletion for any reason.	Data subjects may request deletion for six specific reasons: (1) retaining the personal data is no longer necessary for the purposes for which it was collected; (2) the data subject withdraws consent in accordance with specific GDPR provisions; (3) the data subject objects to the processing pursuant to certain GDPR provisions, and there are no legitimate grounds to overcome the objection; (4) the personal data has been unlawfully processed; (5) the personal data must be erased to comply with a legal obligation in the EU; and (6) the personal data has been collected in relation to the offer of services to a child.
Private rights of action	Limited private right of action for certain data breaches involving combinations of certain data. 30-day cure period for violations. Data subjects may recover the greater of actual damages or statutory damages ($100 to $750 per incident) and seek injunctive and declaratory relief.	Broad private right of action for material or nonmaterial damage caused by a data controller or its service provider's breach of any aspect of the GDPR.

Massachusetts Joint Committee on Consumer Protection and Professional Licensure. If enacted, the law would not take effect until January 2023, after related rulemaking is conducted by the Massachusetts attorney general.

CONCLUSION

The patchwork presented by the laws of these states, along with new laws in Maine, Vermont, and Colorado, is creating a compliance headache for national and international businesses and has many calling upon Congress for a preemptive federal solution.

However, until Congress takes action (which does not appear likely in the immediate future), prudent businesses that wish to operate nationally and globally must prepare to implement privacy compliance programs with at least some state- and country-specific dimensions, despite the laundry list of operational complexities they present and the constantly evolving landscape of state laws.

Endnotes

1. EU General Data Protection Regulation (Regulation 2016/679) (GDPR).
2. GDPR Art. 83. A company's non-compliance with the GDPR could result in fines of up to 4% of its annual global turnover or €20 million, whichever is higher.
3. Cal. Civ. Code § 1798.140(c)(1).
4. Ibid., § 1798.140(c)(2).
5. Ibid., § 1798.144(a)(6).
6. Ibid., § 1798.100(e).
7. Ibid., § 1798.140(t)(2)(D).
8. Ibid., § 1798.140(g).
9. Ibid., § 1798.140(o)(1).
10. California Assembly Bill 874 (AB 874).
11. Ibid.
12. Ibid.
13. California A.B. 25.
14. Ibid.
15. California A.B. 1355.
16. Cal. Civ. Code § 1798.140(o)(2).
17. California A.B. 874.
18. Ibid., §§ 1798.110–125.
19. Ibid., §§ 1798.110; 1798.130.
20. Ibid., § 1798.135.
21. Ibid., §§ 1798.140(v)—(w).
22. Ibid., § 1798.155.
23. Ibid.
24. Ibid., § 1798.150.
25. Ibid.
26. Ibid., § 1798.150(b)(1).
27. Ibid.
28. Ibid.
29. S. 220, 80th Sess. (Nev. 2019).
30. Nevada Revised Statutes, Chapter 603A.
31. S. 120, 191st Sess. (Mass. 2019).

Andrew Baer

andrew@baercrossey.com

Andrew Baer is co-founder and managing partner of the Philadelphia-based law firm of Baer Crossey McDemus. He also chairs the firm's technology and data privacy practice group, where he represents international and Fortune 500 companies as well as emerging growth clients in cutting-edge technology transactions on both the buy and sell sides, cloud computing, data privacy and security compliance (including GDPR, CCPA, and the New York Department of Financial Services Cybersecurity Regulation), copyrights and trademarks, software, digital advertising transactions, and interactive marketing compliance. In 2010, Mr. Baer co-authored the "Corporate Security and Privacy Duties, Policies and Forms" chapter of West's Data Security and Privacy Law Treatise. He holds a JD from University of Chicago Law School and a BA magna cum laude from Dartmouth College, Hanover, New Hampshire.

Matthew Klahre

mklahre@baercrossey.com

Matthew Klahre is an associate in the technology and data privacy practice group at Baer Crossey McDemus. In addition to counseling clients on open-source software licensing and intellectual property protection and infringement, he reviews and negotiates contracts and agreements and advises both large corporate clients and emerging growth companies on software-as-a-service and software licensing, managed services, software and technology development, data privacy and security compliance, lead generation, digital performance marketing, and data licensing. Mr. Klahre obtained his JD summa cum laude from Drexel University, Philadelphia. At Drexel's Thomas R. Kline School of Law, he served as executive editor of articles for the Drexel Law Review and participated in the Entrepreneurial Law Clinic, advising startup clients on technology and intellectual property matters. He also holds a BS from Drexel University.