EQUIPMENT LEASING & FINANCE
FOUNDATION
Your Eye on the Future

CONNECT WITH THE FOUNDATION

JOURNAL OF EQUIPMENT LEASE FINANCING

VOLUME 37 • NUMBER 3 • FALL 2019

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

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

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.

In September 2018, California became the first state to enact commercial financing legislation requiring consumer-style disclosures similar to those required for consumer loans under the federal Truth in Lending Act (TILA) and Regulation Z.[1] Senate Bill 1235, the common shorthand for the new statute referring to its assigned legislation number in the California senate, has been effective for approximately a year, as one of the final acts signed into law by outgoing Governor Jerry Brown. Ever since, commercial lenders have been grappling with how to implement the new disclosure requirements.

Fortunately for many of the affected businesses, S.B. 1235 expressly delayed compliance pending issuance of final regulations by the California Department of Business Oversight (DBO).[2] Nonetheless, many nonbank commercial lenders in the equipment leasing and finance marketplace are bracing for the anticipated sea change this law, along with the inevitable copycat legislation likely to emanate from other jurisdictions, will bring.[3]

This article addresses the requirements imposed by S.B. 1235, explores the policy objectives underlying the legislation, discusses the implications of this legislation for the equipment leasing and finance industry, and it provides practical recommendations for companies to comply.

OVERVIEW OF S.B. 1235

In contrast to the absence of commercial lending regulation in most states, commercial lending has been a regulated activity in California for quite some time.[4] To date, California has primarily regulated finance lenders and brokers engaging in commercial transactions by, among other things, requiring licensure.[5] Although California is not the only state to require licensure for commercial lenders and brokers, it is among the most aggressive in its enforcement of licensure laws for commercial lenders.[6]

However, in recent years concerns have grown that unlicensed lenders were finding new ways to circumvent the requirements by making loans through those exempt from licensure, such as banks.[7] Ostensibly to combat this disparity and to level the playing field, S.B. 1235 will require licensed *and unlicensed* entities (defined as "providers")[8] that extend offers of commercial financing of $500,000 or less to disclose certain information to a recipient at the time the offer is extended, and to obtain the recipient's signature on the disclosure before consummating the commercial transaction.[9]

Significantly, banking institutions themselves remain exempt from S.B. 1235's requirements, while nonbanks bear the burden of compliance with the new law.[10] To that end, a nonbank provider must disclose to the recipient:

- the total amount of funds provided,
- the total dollar cost of the financing,
- the term or estimated term,
- the method, frequency, and amount of payments,
- a description of prepayment policies, and

Editor's Note: This is part 1 of a two-part article. Part 2 will be published in a later issue of the Journal once California's regulations are final. (See endnote 2.)

Because of this narrow definition of a "lease financing," true leases that, for example, either have no end-of-term purchase option or a fair market value purchase option are not subject to S.B. 1235.

- the total cost of the financing expressed as an annualized rate.[11]

S.B. 1235 will also require the foregoing disclosures for two types of products that have not expressly been regulated to date under the California Financing Law: merchant cash advances and factoring.[12] In addition, S.B. 1235 will apply to other accounts receivable purchase transactions, commercial loans, commercial open-end credit plans, and lease financing transactions that the recipient intends to use primarily for *other than* personal, family, or household purposes.[13]

EXEMPTION FOR TRUE LEASES

As noted above, S.B. 1235 applies to a "lease financing," which is defined as a lease for goods "if the lease includes a purchase option that creates a security interest in the goods leased, as defined in paragraph (35) of subdivision (b) of Section 1201 and Section 1203 of the Commercial Code."[14]

Because of this narrow definition of a "lease financing," true leases that, for example, either have no end-of-term purchase option or a fair market value purchase option are not subject to S.B. 1235. As a result, some practitioners have noted that equipment lessors may seek to forgo purchase options on leases in some cases, and may also find it beneficial to shift the process of lease-return sales to auction companies that specialize in such sales.

APPLICABILITY TO BANK SUBSIDIARIES

The DBO's draft regulations exclude nondepository subsidiaries or affiliates from the definition of a depository institution.[15] As a result, if this definition is finalized in the same form, nondepository subsidiaries or affiliates will be subject to S.B. 1235. Notably, this definition would be at odds with the DBO's long-standing position with respect to bank subsidiaries in the commercial lending context.

Specifically, the DBO has previously published regulations clarifying that bank subsidiaries are not exempt from the definition of a finance lender in the context of *consumer* lending, but this limitation on the exemption does not apply in the commercial lending context.[16]

S.B. 1235 also takes aim at banks that partner with financial technology companies to generate loans. The definition of a provider expressly includes a nondepository institution that enters into a written agreement with a depository institution "to arrange for the extension of commercial financing by the depository institution to a recipient via an online lending platform administered by the nondepository institution."[17]

Likely in response to industry concern over the ambiguity of this requirement, the DBO's draft regulations attempt to clarify that the phrase "administered by" excludes an arrangement whereby a nondepository institution provides technology or support services for a depository institution's branded commercial financing program so long as the nondepository institution has no interest, or arrangement or agreement to purchase any interest in the commercial financing extended by the depository institution in connection with such program.

As a result, in some instances, a depository institution's nonbank partner will still be obligated to comply with S.B. 1235's disclosure requirements. Whether a nondepository institution must comply with S.B. 1235 will depend upon whether it "arrange[s]" for the extension of credit through an online lending platform that it administers.

As contemplated by S.B. 1235, it appears that nondepository institutions would not be subject to S.B. 1235 only if: they (1) never present material terms to the applicant, (2) provide only technology or support services to the depository institution's branded commercial financing program, and (3) take no interest in the commercial financing.[18]

While the legislature likely exempted depository institutions because these institutions are already subject to federal regulation, this exemption may nonetheless create additional disparities and costs for nonbanks relative to banks. Further, S.B. 1235 may ultimately have the unintended consequence of limiting entrance into the commercial financing space by requiring nonbanks to comply with significant and costly disclosure requirements.[19]

ADAPTING TO TILA AND REGULATION Z

Unlike TILA, which applies to a subset of consumer financing, S.B. 1235 applies to a variety of divergent commercial financings. Rather than embedding disclosure requirements in the licensing laws that are applicable to each type of financing, the legislature used S.B. 1235 as a vehicle to create an entirely new law to apply substantially the same disclosure obligations to a variety of commercial financings.[20]

However, this approach may somewhat compromise the objective of keeping borrowers informed. For example, the various permutations of commercial financing, developed

specifically to meet the unique objectives of small business borrowers, will likely result in disclosures that are complicated to understand and burdensome to produce.

Furthermore, borrowers may struggle to meaningfully compare disclosures from different types of commercial financing products. For example, the disclosures mandated by S.B. 1235 may not capture the tax and accounting implications or maintenance fees associated with a lease that creates a security interest pursuant to Section 1-203 of the Uniform Commercial Code.

Notwithstanding the differences between TILA and S.B. 1235, some industry members have requested that the DBO commissioner allow for compliance with TILA and Regulation Z for certain types of commercial financings. One commenter advocated for use of the TILA and Regulation Z disclosures.[21]

Other commenters have requested that the regulations adopt certain concepts from TILA and Regulation Z (e.g., annualized rate calculation, establishing tolerance thresholds). However, Regulation Z did not contemplate certain types of products, such as purchasing of accounts receivable or revenue-based loans, which do not have fixed repayment terms. As a result, reliance on TILA and Regulation Z may work for some types of commercial financings but not for others.

In particular, equipment finance industry members may face difficulties in determining how to capture the terms of equipment financings in the disclosures related to the myriad of acquisition costs and fixed and variable payment options typically available under the commercial leases.

The initial draft regulations provide little clarity and indicate only that the provider should calculate the amount of funds provided in one of two ways: (1) if the finance company does not select, manufacture, or supply the goods to be leased, the price the finance company will pay to acquire the property to be leased, or (2) if the finance company selects, manufactures, or supplies the goods to be leased, the price that the finance company would sell the goods in a cash transaction.[22] Absent further direction in the proposed regulations, it appears that equipment financing companies will need to become fluent in the application of Regulation Z in order to determine which types of costs they must include in the finance charge calculation required under the S.B. 1235 disclosures — for example, the cost of insuring the collateral, the cost of filing UCC financing statements, loan commitment fees, and other administrative fees.

CONTINUING CREEP OF CONSUMERISM INTO COMMERCIAL FINANCING

Small business lending has been in the crosshairs of the federal regulatory agenda for years. In 2010, Congress passed Section 1071 of the Dodd-Frank Act, which amended the Equal Credit Opportunity Act to require financial institutions to comply with certain data collection and disclosure obligations in connection with business loan applications.[23]

In 2015, the Federal Reserve Board of Governors and the Federal Reserve Bank of Cleveland published a report studying the impact of online lenders on the small-business credit environment.[24] Among other findings, the report found that, although small business owners initially said it was "easy" to evaluate credit products, when presented with several options, "many expressed uncertainty or answered questions incorrectly when making specific product comparisons, particularly on cost."[25]

Further, many of these small business owners wanted disclosures showing product features and costs in a way that made it easier to compare product offerings.[26] Most recently, the Federal Trade Commission has signaled its desire to regulate the merchant cash advance industry, citing its concern over the "unfair and deceptive marketing, sales and collection practices in the small-business finance market."[27]

The passage of S.B. 1235 offers additional evidence of consumer-style policy priorities and protections creeping into commercial transactions, although this time at the state level.[28] To wit, S.B. 1235 has sparked many comparisons to TILA, which Congress enacted in 1968 to "protect the consumer against inaccurate and unfair credit billing and credit card practices" and "assure a meaningful disclosure of credit terms so that the consumer will be able to compare more readily the various credit terms available to him [and] avoid the uninformed use of credit."[29]

To this end, TILA requires that a creditor disclose "all relevant loan terms," including the amount financed, the finance charge, and the annual percentage rate. Much like TILA's disclosure objectives, the legislature enacted S.B. 1235 with the objective of "help[ing] small businesses better understand the terms and costs of the financing available to them in the commercial financing market."[30]

The passage of S.B. 1235 offers additional evidence of consumer-style policy priorities and protections creeping into commercial transactions, although this time at the state level.

Companies can take certain steps now to begin preparing for the eventual impact of S.B. 1235, including by evaluating their transactions and business models.

STRIKING THE RIGHT BALANCE

While the disclosures mandated by S.B. 1235 are meant to "help small businesses better understand the terms and costs of the financing available to them," ironically, some of the staunchest consumer protection advocates have questioned the efficacy of inundating borrowers with disclosures.[31]

Senator Elizabeth Warren (D-Mass.), a central figure in the Bureau of Consumer Financial Protection's formation, argued against a disclosure-focused regime in a 2010 speech, stating:

> Instead of creating a regulatory thicket of "thou shalt nots," and instead of using ever more complex disclosures that drive up costs for lenders and provide little help for consumers, let's measure our success with simple questions. ... Can customers understand the product, figure out the costs and risks, and compare products in the marketplace?[32]

While some would argue that S.B. 1235's central purpose is to provide the clarity Warren was referring to in her speech, opponents of commercial financing disclosures have an equally valid counterpoint that such a one-size-fits-all view attempts to paint all commercial finance transactions, including complex lease financing with tax, accounting, and strategic planning implications, with a broad brush that likely could cause just the confusion that Warren rails against.

It should go without saying that there is a real risk that more regulation and enforcement efforts, including through disclosures designed to correct purported behavioral market failures, could in fact lead to unfavorable outcomes in commercial lending.[33] But there can be no dispute that many financial products and services suddenly subject to S.B. 1235 have historically been useful and popular among small businesses, in particular, absent the need for legislative or regulatory protections typically reserved for consumer transactions.

KEY TAKEAWAYS AND NEXT STEPS

Companies can take certain steps now to begin preparing for the eventual impact of S.B. 1235, including by evaluating their transactions and business models. For example, a company may:

- Evaluate the commercial financings offered by the company to determine whether these financings would fall under S.B. 1235. This assessment may involve considering the nature of the transactions (e.g., retail installment sale or commercial loan), the purpose of the transactions (e.g., personal or business purpose), and whether these transactions would meet the applicable thresholds.
- Evaluate the disclosures that are currently being provided to customers. This assessment may involve considering the type of information that is contained in these disclosures, the timing in which the disclosures are provided, and how material terms are calculated and presented. Comparing disclosures currently provided with the DBO's draft regulations and sample disclosures may help the company better prepare for compliance with S.B. 1235.
- To the extent the company hosts an online lending platform that arranges for the extension of commercial financing by a depository institution, consider whether the company may be considered a provider of commercial financing subject to S.B. 1235. This assessment may involve evaluating any service agreements with the depository institution to determine whether the services provided could be considered "arrang[ing] for the extension of commercial financing by the depository institution" and whether the company "administer[s]" the online lending platform through which the offer is extended.

CONCLUSION

S.B. 1235 puts commercial lenders and equipment financing companies on notice that potentially burdensome disclosure requirements are on the horizon. In addition to monitoring developments surrounding S.B. 1235, companies should remain apprised of legislative developments concerning commercial financing in other states, as S.B. 1235 will likely continue to serve as a model for future legislation in other jurisdictions.

Endnotes

1. 15 U.S.C. § 1640 et seq; 12 C.F.R. Part 1026.

2. The DBO issued an initial draft of the regulations in July 2019. The regulations are subject to a comment period, after which it is expected that the DBO will issue a revised draft of the regulations. The timing of the revised draft and final regulations is uncertain, but compliance requirements are not expected to be effective until mid-2020 at the earliest.

3. Other states, such as New Jersey and New York, are also moving to regulate small business financing. In New Jersey, the Senate passed a copycat bill in 2018.

4. California enacted the California Finance Lenders Law in 1995, combining three separate licensure laws — the Personal Property Brokers Law, Consumer Lenders Law, and the Commercial Finance Lenders Law — into one. These three laws previously required lenders to obtain three separate licenses to conduct full-service lending in California, including for commercial lending. The California Finance Lenders Law was subsequently renamed the California Financing Law in 2017.

5. See, e.g., Cal. Fin. Code § 22100 ("No person shall engage in the business of a finance lender or broker without obtaining a license from the commissioner."); Ibid. at § 22009 (defining "finance lender" to include any person who is engaged in the business of making commercial loans).

6. Some states have licensure laws that explicitly apply to commercial loans. See, e.g., N.Y. Banking Law § 340 ("No person or other entity shall engage in the business of making loans in the principal amount of […] [$50,000] or less for business and commercial loans, and charge, contract for, or receive a greater rate of interest than the lender would be permitted by law to charge if he were not a licensee […] without first obtaining a license[.]"). Other states have licensure laws that are sufficiently broad so as to capture certain types of commercial loans. See, e.g., S.D. Codified Laws Ann. § 54-4-52 (a license is required to engage in the business of lending money); N.M. Stat. Ann. § 58-15-3(A) (a person must be licensed to engage in the business of lending in amounts of $2,500 or less for a loan.).

7. Senate Comm. on Banking and Fin. Inst., California Financing Law: Commercial Financing: Disclosures at p. 8 (April 16, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180S.B.1235# (noting that S.B. 1235 "attempts to skirt the pre-emption issues that typically plague attempts to regulate bank partnership lending models by placing its disclosure requirements on the nondepository partner rather than the actual bank lender.").

8. Cal. Fin. Code § 22800(m) (defining "providers" as a person who extends a specific offer of commercial financing to a recipient, and also includes "a nondepository institution, which enters into a written agreement with a depository institution to arrange for the extension of commercial financing by the depository institution to a recipient via an online lending platform administered by the nondepository institution. The fact that a provider extends a specific offer of commercial financing or lending on behalf of a depository institution shall not be construed to mean that the provider engaged in lending or originated that loan or financing.").

9. Ibid. at § 22802 (effective *until* January 1, 2024), 22800(n) (defining a "recipient" as a person who is presented a specific commercial financing offer by a provider that is equal to or less than $500,000).

10. Cal. Fin. Code § 22801(a) exempts depository institutions from the disclosure requirements of S.B. 1235, which are defined under § 22800(h) to mean any of the following: (1) A bank, trust company, or industrial loan company doing business under the authority of, or in accordance with, a license, certificate, or charter issued by the United States, this state, or any other state, district, territory, or commonwealth of the United States that is authorized to transact business in this state. (2) A federally chartered savings and loan association, federal savings bank, or federal credit union that is authorized to transact business in this state. (3) A savings and loan association, savings bank, or credit union organized under the laws of this or any other state that is authorized to transact business in this state.

11. Ibid. at § 22802 (effective until January 1, 2024). Effective January 1, 2024, a provider will no longer be required to provide the total cost of the financing, but will be required to provide all other categories of information identified above. Ibid. (effective as of January 1, 2024).

12. Ibid. at § 22800(d)(1). "Factoring" means an accounts receivable purchase transaction that includes an agreement to purchase, transfer, or sell a legally enforceable claim for payment held by a recipient for goods the recipient has supplied or services the recipient has rendered that have been ordered but for which payment has not yet been made. Ibid. at § 22800(i). "Accounts receivable purchase transaction" means a transaction as part of an agreement requiring a recipient to forward or otherwise sell to the provider all or a portion of accounts, payment intangibles, or cash receipts that are owed to the recipient or are collected by the recipient during a specified period or in a specified amount. Ibid. at § 22800(b).

13. Ibid. at § 22800(d)(1). Note also that while S.B. 1235 does not impose any additional disclosure requirements on consumer lending transactions, existing provisions of the California Financing Law require licensed finance lenders to provide certain disclosures to borrowers at the time a consumer loan is made. See, e.g., Cal. Fin. Code § 22337(a); Cal. Code Regs. tit. 10, § 1454.

14. Ibid. at § 22800(j)(1).

15. Cal. Dep't of Bus. Oversight, Proposed Regulations at Cal. Code Reg. tit. 10, § 2057(a)(9).

16. See Cal. Code Regs. tit. 10, § 1422.3.

17. Ibid. at § 22800(m).

18. S.B. 1235 defines a "commercial financing" to mean an accounts receivable purchase transaction, including factoring, asset-based lending transaction, commercial loan, commercial open-end credit plan, or lease financing transaction intended by the recipient for use primarily for other than personal, family, or household purposes. Ibid. at § 22800(d)(1).

19. Apart from depository institutions, S.B. 1235 also provides a limited but specific exemption in connection with recipients that are motor vehicle dealers and vehicle rental companies that receive a specific commercial financing offer or commercial open-end credit plan of at least $50,000. Ibid. at § 22801(d).

20. Senate Comm. on Banking and Fin. Inst., California Financing Law: Commercial Financing: Disclosures at p. 6 (April 16, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180S.B.1235#.

21. Affirm, Re: PRO 01-18 – Comments on Proposed Rulemaking Commercial Financing Disclosures (Jan. 22, 2019), https://dbo.ca.gov/wp-content/uploads/sites/296/2019/04/PRO-01-18-Affirm-Inc.pdf.

22. Cal. Dep't of Bus. Oversight, Proposed Regulations at Cal. Code Reg. tit. 10, § 2066(b).

23. In 2016, we discussed the implications of Section 1071 of Title 10 of the Dodd-Frank Act, which extended certain consumer credit type requirements to business lending and, more broadly, to any entity engaged in financial activity. See John Redding, Moorari K. Shah, Kathleen C. Ryan, and Mitchell M. Grod, "The Impending Impact of Section 1071 and Creeping Consumerism on Equipment Finance," *Journal of Equipment Lease Financing*, vol. 34, no. 1 (Winter 2016).

24. Fed. Reserve Board of Governors & Fed. Reserve Bank of Cleveland, "Alternative Lending through the Eyes of 'Mom & Pop' Small-Business Owners: Findings from Online Focus Groups" (Aug. 25, 2015). In 2018, the Federal Reserve Board and the Federal Reserve Bank of Cleveland expanded on their 2015 study with a subsequent one. See Fed. Reserve Board of Governors & Fed. Reserve Bank of Cleveland, "Browsing to Borrow: 'Mom & Pop' Small Business Perspectives on Online Lenders" (June 2018), https://www.federalreserve.gov/publications/files/2018-small-business-lending.pdf. According to the 2018 survey, numerous participants noted that even though a borrower's actual interest rate may vary, "they wanted at least some information upon which to compare options and to make decisions on whether to apply." Ibid. at 14.

25. Ibid. at 3.

26. Ibid.

27. See Zachary R. Mider, "FTC Commissioner Calls for Review of Small-Business Loan Practices," *Washington Post* (May 9, 2019), https://www.washingtonpost.com/business/on-small-business/ftc-commissionercalls-for-review-of-small-business-loan-practices/2019/05/08/149b8650-71a9-11e9-9331-30bc5836f48e_story.html?utm_term=.93d545d80433.

28. New Jersey's S.B. 2262 would impose certain disclosure obligations on an entity (whether a bank or nonbank) that provides a commercial loan in the amount of $100,000 or less to a small business located in New Jersey. S.B. 2262, New Jersey (2018-2019). It would require a covered entity to disclose information such as the annual percentage rate, the interest rate, the finance charge, the amount financed (for a term loan), the borrowing limits (for a revolving credit loan), and any third-party agreements entered into between the entity that provides the small business loan and any broker or other third party involved in the loan. In New York, S5470 was recently referred to the Committee on Banks. See S5470, New York (2019-2020). The bill would also require disclosure of certain terms, such as the amount financed and total cost of the financing. Ibid. In

contrast with California's S.B. 1235, S5470 takes a more nuanced approach by providing disclosure requirements for certain types of commercial financings (e.g., accounts receivable purchase, closed-end commercial financing). Ibid.

29. 12 C.F.R. § 1026.1(b); 15 U.S.C. § 1601(a).

30. Commercial Financing: Disclosures Report, California Senate Committee on Banking and Financial Institutions (Aug. 31, 2019), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180S.B.1235#.

31. Senate Comm. on Banking and Fin. Inst., California Financing Law: Commercial Financing: Disclosures at p. 4 (April 16, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180S.B.1235#.

32. David Lawder, "Consumer Czar Warren Says Wants Banks' Help on Rules," Reuters (Sept. 28, 2010), https://www.reuters.com/article/us-financial-warren/consumer-czar-says-wants-banks-help-on-rules-idUSTRE68T0AB20100930.

33. Jialan Wang and Benamin J. Keys, "Perverse Nudges: Minimum Payments and Debt Paydown in Consumer Credit Cards," Wharton Univ. of Penn: Public Policy Initiative, vol. 2, no. 4 (April 2014), https://publicpolicy.wharton.upenn.edu/issue-brief/v2n4.php.

Clinton R. Rockwell

crockwell@buckleyfirm.com

Clinton Rockwell is the managing partner of Buckley LLP's Los Angeles and San Francisco offices. He advises clients nationwide on consumer financial services matters, including private equity, banks, mortgage companies, fintech lenders, commercial lenders, secondary market loan purchasers, and securities broker-dealers, including regulatory, licensing, compliance, and transactional matters. Mr. Rockwell's work also includes advising on California-specific lending matters, including the California Finance Lenders Law. He was one of the original members of Buckley Kolar LLP, joining the firm as an associate at its formation in 2004. Prior to joining Buckley, he was with Goodwin Procter LLP in Washington, DC. Mr. Rockwell received his JD from George Washington University, Washington, DC; his LLM from University College London; and his BA cum laude from the University of California, San Diego.

Kathryn L. Ryan

kryan@buckleyfirm.com

Kathryn Ryan is a partner in Buckley LLP's Washington, DC, office. She advises financial services companies on various regulatory, licensing, compliance, and transactional matters. These include federal and state compliance requirements, Secure and Fair Enforcement (SAFE) Act compliance, Federal Housing Administration compliance, and the risks associated with the False Claims Act and the Financial Institutions Reform, Recovery and Enforcement Act (FIRREA). Ms. Ryan's clients include banks, first and second mortgage originators, reverse mortgage originators and services, fulfillment service providers, commercial lenders and servicers, bank holding companies, private equity firms, finance companies, debt collection companies, financial institutions and technology companies, payment processors, and money transmitters. Ms. Ryan received her JD from Catholic University of America in Washington, DC, and her BA from the University of Virginia in Charlottesville.

Moorari K. Shah

mshah@buckleyfirm.com

Moorari Shah serves as counsel in the Los Angeles office of Buckley LLP. He represents banks, fintechs, mortgage companies, auto lenders, and other nonbank financial institutions in transactional, licensing, regulatory compliance, and government enforcement matters. His work covers mergers and acquisitions, consumer and commercial lending and leasing, equipment finance, and supervisory examinations and enforcement actions involving state and federal agencies. Mr. Shah regularly advises companies on California-specific financing topics, including new legislation affecting consumer and commercial lenders and lessors as well as matters before the California Department of Business Oversight. This year, the Equipment Leasing and Finance Association awarded him its David H. Fenig Distinguished Service in Advocacy Award. Mr. Shah received his JD cum laude from Boston University School of Law and his BA from Duke University in Durham, North Carolina. He is a certified information privacy professional and a certified Six Sigma Black Belt.

Frida Alim

falim@buckleyfirm.com

Frida Alim is an associate in the Los Angeles office of Buckley LLP. She assists clients in regulatory and compliance matters and provides support for complex litigation and government investigations involving the mortgage lending industry. Previously, she worked at an intellectual property litigation firm in San Francisco. As a fellow at the Electronic Frontier Foundation, Ms. Alim worked on data privacy matters. While in law school, she served as symposium editor for the *Berkeley Journal of International Law*. She received her BA from the University of California, Berkeley.

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.

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.

Blockchain is set to revolutionize recordkeeping and securitization across the private sector in the United States and abroad, including commercial lending and the equipment finance space. The potential benefits in efficiency, cost reduction, and convenience are enormous and are rapidly being implemented in the private sector. However, for a variety of reasons, the public and private sectors are often out of step when it comes to implementing new technology. Are the two sides able to find common ground?

State governments at all jurisdiction levels have struggled to meet the sometimes unrealistically high standards of citizens and businesses around their concerns for security, access, and high-quality maintenance of public and private information. Modern technology has created the expectation of immediate feedback and results, but that is not always reality.

For instance, it can take several days for a bank to determine via state and local governments if a business that has applied for a loan has already mortgaged the same collateral with another lender. An individual trying to rectify a faulty land record will sometimes need to navigate several touchpoints to get the information corrected.

States also face enormous challenges in establishing transparency in governance processes, given the realities of public budgets and sometimes incompatible technology platforms. The side effects can include manual work processes, duplication of effort, errors in data entry due to manual recordation, handoffs in processes, and specialized resources to handle critical data.

This, in turn, drives higher costs, longer cycle times for servicing citizens and businesses, and poor service levels. Further, like every other individual and entity connected to the internet, state and local jurisdictions are increasingly under attack by hackers, raising concerns over the security of these systems.

Accordingly, commercial lenders and businesses must work together with state and local governments for the benefit of all their respective constituents. These constituents are very similar to those constituencies in for-profit institutions. In business we know that increased employee satisfaction leads to greater customer satisfaction — which leads to shareholder value in the public sector.

These constituents include all of the employees that work for the public jurisdiction, the "customers" that use the system, and all of the public entities and their taxpayers that use their systems. It is imperative that all implementations of new systems serve the interests of all these constituencies.

Public records are the cornerstone of UCC filing in the equipment finance sector and, by extension, profitability for equipment financers. For governments, improving the current state with existing systems and technology is a challenge due to complex in-place purchasing policies and constrained budgets.

Blockchain has the potential to help states establish and demonstrate transparency, speed up processing times, and cut operational costs related to

Adopting blockchain promises transparency in governance and allows for both secure transactions and accurate recordation at reduced costs.

commercial lending. In this light, it is encouraging to see some states accepting, experimenting with, and adopting blockchain for public recordkeeping at this early stage in the blockchain technology life cycle. But what does that mean for equipment finance?

BLOCKCHAIN AS A TECHNOLOGY FOR GOVERNMENTS CAN TRANSFORM THE FINANCIAL SECTOR

Blockchain is a distributed ledger database with multiple stakeholders on its network. It digitally records data for every transaction in chronological order in the form of "blocks" and creates a "chain" of blocks linking subsequent transactions to the previous ones. Each block is immutable, contains details of transactions and descriptions, and provides transparency to users that can view the digital block.

The technology promises to be highly secure and almost impossible to tamper with because the blockchain ledger is replicated on servers on a global scale and is easily accessible by users. Moreover, it allows for provenance, allows tracking of chain of custody, and ensures accuracy.

Specifically, blockchain can establish security around recordation, access, and authentication for maintaining personal, public, and corporate data; asset ownerships; trading and exchange of assets; cross border business regulations; enforcement of smart contracts; and digital signature authentication.

Blockchain can also make the due-diligence and risk assessment much faster with "KYC" (know your customer) due diligence requirements. As the information about businesses and their corporate information moves from paper and the web (stored in government and other corporate records) to the blockchain, it will be much faster to conduct the search for business names and corporate profiles, including outstanding liens and any adverse records.

As a result, lenders will be able to conduct due diligence much faster than they do today. Clearly, where lenders can conduct due diligence easily, they will be more apt to do business. This benefits everyone involved with the transaction.

Blockchain can also help build "smart UCCs" that automate the entire life cycle of filings. The process may not require any manual action for the filing, as long as the business logic can be embedded in the filing itself through blockchain's smart contract mechanism. This would automate any future actions for the filing including amendments, renewals, and terminations. The operational cost savings for both the states and lenders would, in theory, be quite significant.

STATE GOVERNMENTS ARE EXPLORING THE TECHNOLOGY FOR SEVERAL REASONS

State governments have started looking at blockchain as a way to reduce costs and improve transparency for their regulatory filings and public data. It is only a matter of time before banks and other financial institutions will be able to leverage state-held public information like UCC and corporate charter information, land records, and motor vehicle titles to make lending decisions faster and also monitor the risk to their loans through tracking services.

Faster approvals are in everyone else's interest as well: the customer gets faster turnaround, the workload is reduced for public employees, and costs are reduced for states and municipalities.

States are also concerned about protecting revenues, given that states act as middlemen, charging a transaction fee for recordation and access. It is conceivable that the public sector is vulnerable to private parties that might provide a more efficient blockchain-based service, thereby cutting states out of a valuable revenue stream.

Some states have been early and enthusiastic experimenters with blockchain. To date, at least 16 states are in some stage of adopting blockchain: Arizona, California, Delaware, Florida, Hawaii, Illinois, Maine, Maryland, Michigan, Nebraska, New Jersey, New York, Ohio, Tennessee, Vermont, and Wyoming.

In addition to the benefits of reducing costs and increasing the accuracy of public records, states are looking to improve their ease of doing business in order to attract new businesses to incorporate in their state. Adopting blockchain promises transparency in governance and allows for both secure transactions and accurate recordation at reduced costs. These benefits could easily make a state more attractive to new businesses.

However, states still need to carefully consider how they legitimize, regulate, pilot, adopt, and scale the technology. There are five stages of this adoption journey, outlined as follows:

1. Exploration – where states form a task force; carefully consider their specific needs; assess the impact, benefits and risks; publish findings; invite opinions from industry players, technology partners, and citizens; and make recommendations to the appro-

In the medium term, competition among states to attract new businesses and a fear of losing existing revenue are pushing states to act.

priate elected officials and relevant regulatory agencies.

2. Legislation – where states enact laws to recognize use of blockchain technology for a specific purpose, legitimize the records held on blockchain in a court of law, create safeguards against misuse, and incentivize innovation.
3. Pilot – where a state engages with technology partners to build prototypes, pilot the use for specific use cases, and learn from feedback.
4. Early Adoption – where states adopt the use of blockchain with use cases with specific objectives. Delaware and Ohio are moving toward early adoption. Delaware had its first milestone in 2016 when the state authorized tracking of share issuances and transfers on blockchain and smart contracts. In 2017, the state initiated a pilot for "Smart UCC filing," exploring automated release or renewal of UCC filings and faster and efficient searching of UCC records. Delaware is now piloting blockchain-based business filing. In Ohio, Franklin County is working with a real estate blockchain startup and plans to move all its land parcels onto a digital ledger in the next three years (2019–2022). Earlier in 2018, Franklin County also auctioned off 36 forfeiture properties by transferring the deeds via the Ethereum blockchain.
5. Transformation – where states adopt the technology across multiple areas of governance such as individual and property records, titles, liens, real estate records, supply chain tracking, electronic records, contract execution, business and asset registrations, and digital signatures.

Government adoption will accelerate once a state has success in scaling a blockchain initiative, and there is movement toward a light touch and progressive regulatory environment. This will enable blockchain-based innovation, possibly leading to an open market for applications built for states.

BARRIERS TO BLOCKCHAIN ADOPTION BY STATES

On the technology front, lack of agreed-upon standards, interoperability across blockchain platforms, and maturing the technology in terms of scalability and processing power will need to be dealt with and overcome. Having enough experienced talent to deliver blockchain solutions is another issue — a challenge of varying degrees depending on the state in question. Recent advances in ledger-agnostic (non-ledger-specific) blockchain technology and common standards across blockchain consortia will help address some of these key technological challenges.

There are other, nontechnical barriers to the wide implementation of blockchain in government bodies. These include the different processes and purchasing procedures at each level of government to create requests for proposals, "hidden stakeholders" that can introduce delays and complexity in the bidding and specification process, complications from public employee employment contracts, and the need for public hearings and comments that may emerge from these.

In the short term, governments are likely to continue to explore the potential of blockchain technology. In the medium term, competition among states to attract new businesses and a fear of losing existing revenue are pushing states to act. Successful pilots across a range of use cases nationwide should establish the viability of the technology.

Movement by an early adopter state will likely trigger a wave of adoption from other states. However, this situation poses the significant challenge of different vendors selling incompatible systems to various states. Any of these could compromise the efficiency of blockchain for all users.

KEY TAKEAWAYS

Lack of knowledge about blockchain among lawmakers, resistance to change, lack of standards across blockchains, and lack of interoperability are key barriers to blockchain adoption by states.

Given the transformative benefits for states and local government, and the challenges to adoption, strong sponsorship by elected officials and excellent implementation team leadership will be crucial to the first successful implementation at scale.

Once one state crosses the threshold beyond the pilot phase and into the early adoption phase, competition among states to attract new businesses will create the necessary snowball effect. The state that executes the early adoption phase and plans for broad adoption of blockchain technology as part of a transformation phase will draw investors and attract new businesses and investments to that state.

Regardless, financial organizations and states are continuing their long journey toward collectively adopting blockchain. At the end of the day, governance will be transformed.

Raja Sengupta

raja.sengupta@wolterskluwer.com

Raja Sengupta is executive vice president and general manager of Wolters Kluwer's Lien Solutions in Houston. As the chief executive of the business, Raja leads a growing organization focused on providing search and filing services through its nationwide network. Before joining Lien Solutions, Mr. Sengupta was executive vice president and general manager of CT Small Business, a Wolters Kluwer business providing compliance solutions to small and midsized businesses for business formations, business license, digital brand protection, and other issues relating to governance, risk, and compliance. He has deep roots in the financial services world as well as broad experience in leveraging technology and organizational and process redesign to reveal commercial opportunities and increase value in organizations. Mr. Sengupta received a BS in technology from the Indian Institute of Technology in Kharagpur and an MBA from the Indian Institute of Management in Bangalore.