

THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018: TOUGHEST U.S. DATA PRIVACY LAW WITH TEETH?

*Yunge Li**

INTRODUCTION

Despite numerous efforts by industry groups and tech companies over the past several months to water down¹ and ultimately halt² the first-ever U.S. data privacy law, the California Consumer Privacy Act of 2018 (“CCPA” or “the Act”), now has its language finalized as of September 13, 2019, the end of California’s legislative calendar, and is slated to go into effect on January 1, 2020.³ The goal of the Act is to give California residents greater control over the personal data companies collect and process.⁴

The CCPA focuses on transparency, control, and accountability.⁵ Under the new law, California residents will now have the right to learn what personal data is being collected by companies like Facebook and Google, they will have a way to stop the sharing or selling of personal information, and they will have the ability to sue

* Loyola University Chicago, Juris Doctor Expected 2021, Staff Editor, Consumer Law Review

¹ See *A Watered-Down Version of California’s Data-Privacy Law is A Possibility, Privacy Experts Warn*, MARKET WATCH, <https://www.marketwatch.com/story/a-watered-down-version-of-californias-data-privacy-law-is-a-possibility-privacy-experts-warn-2019-06-27>.

² See Alfred Ng, *Tech Giants Ask Congress for Data Privacy Bill to Bypass State Laws*, CNET, (Sep. 10, 2019), <https://www.cnet.com/news/tech-giants-ask-congress-for-a-data-privacy-bill-that-would-bypass-state-laws/>.

³ Deborah A. George, *California CCPA Amendment Update: Here’s What Passed*, THE NATIONAL LAW REVIEW (Sep. 19, 2019), <https://www.natlawreview.com/article/california-ccpa-amendment-update-here-s-what-passed>.

⁴ See *About Us*, CALIFORNIANS FOR CONSUMER PRIVACY, <https://www.caprivacy.org/about-us> (last visited Oct. 15, 2019).

⁵ *Id.*

over data breaches or privacy violations if companies fail to comply with the CCPA.

Specifically, the rights conferred to consumers include: the right to know what personal information businesses are collecting about them and how that information is being used and shared, the right to delete personal information held by the business, the right to reject the selling of personal information and the right to non-discrimination in services and price when exercising privacy rights.⁶ With a good-faith intent to empower the consumer, the law introduces a potential threat of fraudulent requests⁷ when individuals try to abuse the right of access since the definition of a verifiable consumer request was not clearly defined in the text.⁸

The Act aims to broadly expand the rights of consumers while requiring businesses within the scope to be significantly more transparent about how they collect, use, and disclose personal information.⁹ Despite having serious consequences, businesses are moving slowly in their compliance preparations.¹⁰ A recent survey conducted by PricewaterhouseCoopers shows that 52% of respondents are planning to be compliant by January 2020. Most of the companies were concerned that the Act is too vague and broad, making the implementation difficult and complicated.¹¹ For instance, what constitutes a “sale”¹² of personal data? How do you reasonably verify the consumer identity? What level of deletion is required? These are just a few of many questions regarding the ambiguities in the CCPA that companies scramble as they seek legal advice to comply.

The Article is organized in five parts. Part II reviews the United

⁶ *About the Law*, CALIFORNIA'S FOR CONSUMER PRIVACY, <https://www.caprivacy.org/about-us> (last visited Oct. 15, 2019).

⁷ Joe Uchill, *Hacking the Vulnerabilities in Privacy Laws*, AXIOS, (Jul. 11, 2019), <https://www.axios.com/privacy-law-europe-gdpr-companies-personal-data-e7330ab1-5d7c-431b-a9b3-b4f81c7fbf53.html>.

⁸ Annie Bai & Peter McLaughlin, *Why CCPA's 'Verified Consumer Request' is A Business Risk*, IAPP, (Aug. 14, 2019), <https://iapp.org/news/a/verified-consumer-request-dont-naively-slip-into-the-crack-or-is-it-a-chasm/>.

⁹ *See Supra* note 4.

¹⁰ Patience Haggin, *Businesses Across the Board Scramble to Comply with California Data-Privacy Law*, WSJ, (Sep. 8, 2019), <https://www.wsj.com/articles/businesses-across-the-board-scramble-to-comply-with-california-data-privacy-law-11567947602>.

¹¹ *Id.*

¹² *California Consumer Privacy Act of 2018*, CAL. CIV. CODE § 1798.140 (t), (2018) (effective Jan. 1, 2020); *See* Lydia de la Torre & Sebastiano Rupp, *What Does 'Valuable Consideration' Mean Under the CCPA*, IAPP, (Dec. 6, 2018), <https://iapp.org/news/a/what-does-valuable-consideration-mean-under-the-ccpa/>.

2019]

Desktop Publishing Example

167

States legislative and regulatory environment on consumer data-privacy protection. In addition, it identifies California at the privacy vanguard to protect consumer privacy rights. Part III describes the CCPA passage. It follows the history of a citizen-funded ballot initiative transforming into a state-sponsored privacy bill and lays out the legal backdrop for the bill. It also highlights how different interest groups wrestled with each other throughout the passage of the bill. Part IV discusses in-depth what privacy rights have been conferred to the consumer and how the California Attorney General plans to enforce the Act. Part V identifies key operational obstacles that could weaken the Act's original purpose. Part VI concludes the Article by discussing the impact of the CCPA on a national level.

THE U.S. CONSUMER DATA PRIVACY PROTECTION

A. Common Law and the Constitution

Historically, the common law in the United States protects privacy fixed on an object, such as property rights against trespassing, but little was said about rights to personal privacy.¹³ In 1890, Samuel Warren and Louis Brandeis published a groundbreaking article which introduced the concept of “right to privacy” and “the right to be left alone.”¹⁴ Later, with the development of social environment and technology, demands on individual privacy grew.¹⁵ Yet privacy revolved more around tort law – often under the doctrines of intrusion, public disclosure, or appropriation.¹⁶ Accordingly, the Constitution has now been interpreted to create a right to privacy which is designed to assure that the minds and property of Americans remain free from government intrusion.¹⁷ For example, the fourth amendment guarantees “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”¹⁸

Until today, the United States still lacks a single, comprehensive federal law that regulates the collection and use of personal information.¹⁹ Instead, the government has approached

¹³ Daniel J. Solove, *A Brief History of Information Privacy Law*, in PROSKAUER ON PRIVACY § 1-4 (2006) (citing David H. Flaherty, *Privacy in Colonial New England* 1 (1972)).

¹⁴ 4 HARV. L. REV. 193, 195-6 (1890).

¹⁵ *See Supra* note 13.

¹⁶ Solove, *supra* note 13, § 1-14.

¹⁷ U.S. CONST. amend. III.

¹⁸ *Id.* amend. IV.

¹⁹ Chris D. Linebaugh, et. el., *Data Protection Law: An Overview*,

privacy and security by regulating only certain sectors and types of sensitive information (i.e., protected health information under the Health Insurance Portability and Accountability Act (“HIPAA”)²⁰, student information under Family Educational Rights and Privacy Act (“FERPA”) of 1974²¹ and financial information under Gramm-Leach-Bliley Act²²), oftentimes creating overlapping and contradictory protections. All of the current constitutional rights protecting privacy focus on public disclosure of private facts.²³ This focus purely on the dispatch on information after it’s acquired limits its potential influence on modern data privacy debates, which extends beyond disclosure, and more broad concerns about how data is collected, processed, and used.²⁴ Since neither common law and the Constitution grants a comprehensive framework to protect consumer data privacy, a more stringent standard should come from the statutory law.

B. California at the Consumer Privacy Vanguard

California has pioneered the codification of privacy protections in the United States. In 1972, the California Constitution was amended to include the right of privacy among “inalienable” rights of all people.²⁵ In 2002, California Legislature requires any company that stores customer data electronically to notify its California customers of a security breach to the company’s computer system if the company knows or reasonably believes that unencrypted information about the customer has been stolen.²⁶ From 2002 through 2017, California Legislature enacted privacy related laws including: California Data Breach Notification Law, Online Privacy Protection Act, Shine the Light Law, Privacy Rights for California Minors in the Digital World Act, and California

Electronic Communications Privacy Act.²⁷ In the section

CONGRESSIONAL RESEARCH SERVICE, (Mar. 25, 2019).

²⁰ P.L. 104-191.

²¹ 20 U.S.C. § 1232g.

²² 113 STAT. 1338.

²³ *Supra* note 19.

²⁴ Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law*, 564 (6th ed. 2018).

²⁵ The California Constitution provides that all people are by nature free and independent and have inalienable rights. Among there are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (CAL. CONST., ART. I, SEC. 1.)

²⁶ 2002 Legis. Bill Hist. CA S.B. 1386.

²⁷ CAL. CIV. CODE §§ 1798.29; CalOPPA, CAL. BUS. & PROF. CODE §§ 22575-22579 (2004); “Shine the Light” law is considered one of the first attempts by a state

2019]

Desktop Publishing Example

169

below, the article will discuss two of California pioneer privacy protection laws in understanding how California stays at the forefront of consumer privacy protection.

1. California Data Breach Notification Law

California lawmakers have displayed how seriously they take the privacy of Californian citizens. Privacy is an inalienable right granted under the California Constitution.²⁸ California was the first state to enact laws protecting the rights of its residents to be notified in the event of a data security breach.²⁹ Soon forty-eight states followed and implemented their own data breach notification law, all of which were modelled off of California's.³⁰ But, California remains one of the few states that require the entity to provide credit monitoring services or identity theft protection after financial information is compromised.³¹ This requirement provides extra layer of protection on consumer privacy because identity theft accounted for over 42 percent of all frauds reported to federal authorities.³²

2. California Electronic Communications Privacy Act

On January 1, 2016, the landmark California Electronic Communications Privacy Act ("CalECPA") went into effect.³³ It was hailed as "the nation's best privacy law" at that time.³⁴ Under CalECPA, no California government entity can search California residents' phones and online accounts without obtaining a warrant for cause.³⁵ The legislation has two main parts: a warrant requirement and

legislature in the United States to address the practice of sharing customers' personal information for marketing purposes, also known as "list brokerage," CAL. CIV. CODE § 1798.83; Privacy Rights for California Minors in the Digital World, CAL. BUS. & PROF. CODE §§ 22580-22582 (2013); CalECPA, CAL. CIV. CODE § 1798.82.

²⁸ *Supra* note 21.

²⁹ CAL. CIV. CODE §§ 1798.29(a), 82(a).

³⁰ *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS, (Jan. 30, 2018), <https://www.cfr.org/report/reforming-us-approach-data-protection>.

³¹ *Supra* note 25, §1798.82.

³² Why Credit Monitoring? FORBES, <https://www.forbes.com/credit-center/why-credit-monitoring.html> (last visited Nov. 18, 2019).

³³ *Id.*

³⁴ *California Electronic Communications Privacy Act (CalECPA) - SB 178*, ACLU NORTHERN CALIFORNIA, (updated April 2018), <https://www.aclunc.org/our-work/legislation/calecpa>.

³⁵ *Id.*

a notice requirement. While federal law already requires a warrant to acquire electronic communication content, CalECPA provides both mandatory and discretionary means for judges to confine warrants *only* to relevant information.³⁶ It requires notice to the target, even in emergencies, and even when the targets may not be identified, although notice may be delayed in limited cases.³⁷

THE PASSAGE OF THE CCPA

This U.S. version of General Data Protection Regulation (“GDPR”)³⁸ was introduced roughly a year after the EU privacy law was enacted. It was designed to be a similar, though not identical mechanism, to regulate consumer privacy. The initiative was brought by Alastair Mactaggart, a wealthy San Francisco real-estate developer who was disturbed by the lack of data privacy protections from after chatting with a Google engineer at a cocktail party.³⁹ The bill was passed unanimously by California lawmakers⁴⁰ and was signed into law by Governor Jerry Brown on June 28, 2018.⁴¹ Since the enactment, California lawmakers introduced a series of bills to help further clarify and refine the scope of the Act.⁴²

A. The Ballot Initiative and Legislative History

Originally, Alastair Mactaggart, the main architect and sponsor of the initiative,⁴³ spent nearly \$3.5 million to promote and place a

³⁶ *Id.*

³⁷ *Id.*

³⁸ *GDPR Key Changes*, EU GDPR.ORG, <https://eugdpr.org/the-regulation/> (last visited Nov. 18, 2019).

³⁹ *See Supra* note 4.

⁴⁰ Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED, (Jun. 28, 2018), <https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/>.

⁴¹ *Governor Brown Signs Landmark Privacy Law*, CAL. SENATOR BILL DODD, (Jun. 28, 2018), <https://sd03.senate.ca.gov/news/20180628-governor-brown-signs-landmark-privacy-law>.

⁴² Ashley Shively, *California Privacy Act Update, Assembly Approves 12 Amendments - Changes Would Exclude Employees and Vehicle Information, Protect Loyalty Programs*, JDSUPRA, (Jun. 7, 2019), <https://www.jdsupra.com/legalnews/california-consumer-privacy-act-update-48943/>.

⁴³ *The Consumer Right to Privacy Act of 2018 Initiative*, (Nov. 17, 2017), <https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf>.

2019]

Desktop Publishing Example

171

consumer data privacy initiative on California's November ballot. Because California allows laws to be adopted by the voters in addition to the legislature, the initiative was put on the ballot by more than 600,000 signatures from voters.⁴⁴ The privacy ballot initiative has restrictive language empowering the California consumer in a way that businesses trafficking in big data would not want to see.⁴⁵ Before the privacy initiative went on the ballot, California legislators worked with representatives of affected California businesses and other interest groups, and quickly negotiated a deal with Mactaggart in exchange for the passage of a substantially similar law, leaving his opponents with unpopular and expensive campaigns.⁴⁶

This agreement was announced publicly less than a week before the California Legislature rushed the bill through both houses, which it did just hours before the Thursday deadline for Mactaggart to withdraw his measure from the ballot.⁴⁷ The bill – the California Consumer Privacy Act of 2018 successfully passed both houses with majority votes and was signed into law by California Governor Jerry Brown.⁴⁸

B. Amendments and Regulations

The CCPA passed with aggressive language and ambiguous terms in a rush to avoid competing versions, the California Legislature was expected to amend the CCPA.⁴⁹ Notably, the California AG's

⁴⁴ See *History of the CCPA*, CLARIP, <https://www.clarip.com/data-privacy/california-consumer-privacy-act/> (last visited Oct. 15, 2019).

⁴⁵ See *AB 375 Privacy: Personal Information: Businesses Oppose – As Amended June 25, 2018*, (Jun. 27, 2018), https://nrf.com/sites/default/files/imported_files/imported_files_other/DataPrivacy-2018-California-AB%20375%20Floor%20Letter%20Oppose.pdf. Arguments in opposition from a coalition of businesses and organizations: “We are now faced with a “take it or leave it” scenario which is very problematic given that the business community overall has had little input to these negotiations. Even more troublesome, the newest amendment expanding the liability in what is supposed to be the “data breach” section of this bill has nothing to do with privacy.

⁴⁶ *An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy*, 2017 Legis. Bill Hist. CA A.B. 375, https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited Oct. 15, 2019).

⁴⁷ *Supra* note 39.

⁴⁸ *Supra* note 42.

⁴⁹ Alan Friel, *Preparing for California's New Privacy Law Will Make for a Busy 2019 for Legal, IT and Info Governance Departments*, BakerHostetler, <https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/Friel-AMEC.pdf> (last visited Oct 15, 2019).

Office had expressed five primary concerns with the existing language in the CCPA.⁵⁰ On August 21, 2018, the Legislature passed SB 1121, a small technical amendment that did not make any necessary changes to some of the overbroad definitions of the Act. Since it passed, there have been additional calls for amendments both by the bill's supporters, consumer organizations, and business organizations.⁵¹

The enactment of CCPA sparked intense focus on privacy regulation at the State level. California's state legislature alone introduced over one hundred privacy bills in 2019, with the majority proposing changes to CCPA. September 13, 2019 marked the deadline for any amendments to be approved by the houses. Only five of these bills made it past the state senate.⁵² Industry-backed amendments relating to loyalty programs, targeted ads, or the expanded definition of de-identified data did not pass. On October 11, 2019, California Governor Gavin Newsom signed all five of the California Legislature's amendments to CCPA into law.⁵³

THE CCPA CONSUMER PRIVACY RIGHTS

The California Attorney General ("AG") announced Proposed Regulations implementing the CCPA on October 10, 2019.⁵⁴ According to the AG, "The proposed regulations would establish procedures to facilitate consumers' new rights under the CCPA and

⁵⁰ Xavier Becerra, *RE: California Consumer Privacy Act of 2018*, (Aug. 22, 2018), https://iapp.org/media/pdf/resource_center/AG-Ltr-CaCPA-8-22-2018.pdf. In the letter, the AG stated that his office should act as an enforcer rather than regulator. The AGO's five concerns related to: Consultation, Civil penalties, Notification of lawsuit, AG regulation timeframe and the private right of action.

⁵¹ *Business Community Requests to be Included in AB 375 Clean-up Legislation*, (Aug. 6, 2018), <https://regmedia.co.uk/2018/08/21/ca-privacy-act-big-tech.pdf>. Coalition of 30 plus industry associations and groups, including CA Chamber of Commerce, advocated for modifications and clarification of the bill.

⁵² AB 1355 (clarifies breach provision and makes changes to some basic definitions); AB 25 (Partially excludes employee information at least in 2020); AB 1146 (Exempts vehicle and ownership information); AB 1564 (toll-free number alternative); and AB 874 (clarifies exemptions from the definition of "personal information").

⁵³ *Governor Newsom Issues Legislative Update 110.11.19*, OFFICE OF GOVERNOR GAVIN NEWSOM, <https://www.gov.ca.gov/2019/10/11/governor-newsom-issues-legislative-update-10-11-19/>.

⁵⁴ *Press Release*, XAVIER BECERRA ATTORNEY GENERAL, (Oct. 10, 2019), <https://www.oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california>.

2019]

Desktop Publishing Example

173

provide guidance to businesses for how to comply.”⁵⁵ These regulations are intended to operationalize the CCPA into a fully functional process and provide clarity and specificity to assist the implementation of the law. The following sections will look at the privacy rights conferred to the consumers and whether AG’s proposed regulations add clarity to protect the consumer privacy rights.

A. Applicability

The CCPA applies to any for-profit business that handles “personal information” about a consumer, and satisfies at least one of the following thresholds: (1) has annual gross revenues in excess of \$25 million; (2) possesses the personal information of 50,000 or more consumers, households, or devices; **or** (3) earns more than half of their annual revenue from selling consumers’ personal information.⁵⁶ Even companies with no physical presence in California but a website that serves Californians are required to comply.

The CCPA defines consumer as a natural person who is a California resident.⁵⁷ While the Act strives to hold larger corporations accountable when handling California residents’ personal data, it might have detrimental effects on some of the smaller businesses. Local business owners were worried about the heavy burden and cost of implementing a comprehensive compliance program.

B. Right to Know

The first section of the Act provides consumers the right to access their personal information.⁵⁸ Under the law, consumers have the right to demand disclosure of any of their personal information a business has collected, no more than twice within a 12-month period.⁵⁹ At or before the point of collection, a business has to inform consumers as to the categories of information collected from them and the purposes for which it will be used.⁶⁰ Privacy notices must also be provided at or before point of collection, explaining, in plain and straightforward language, consumers’ privacy rights and methods for submitting requests.⁶¹ Upon a verifiable consumer request, the

⁵⁵ *Id.*

⁵⁶ CAL. CIV. CODE § 1798.140 (c) (2018)

⁵⁷ CAL. CIV. CODE § 1798.140 (g) (2018)

⁵⁸ CAL. CIV. CODE § 1798.100. (2018)

⁵⁹ *Id.* § 1798.100(d).

⁶⁰ *Id.* § 1798.100(b).

⁶¹ *Id.*

business has to disclose (1) the specific pieces of personal information the business has collected about the consumer; (2) categories of personal information it has collected or sold about that consumer; (3) the purpose for which it collected or sold the categories of personal information; and (4) categories of third parties to whom it sold the personal information.⁶² The disclosure should also include the categories of personal information the business sold to third parties.⁶³

C. Right to Delete

Consumer has the right to request deletion of any personal information a business collects.⁶⁴ Businesses within the scope of the Act are required to inform the consumer that deletion is available to her.⁶⁵ Upon a verifiable consumer request, the business is required to delete the information from its records and direct any service providers to comply with deletion.⁶⁶ However, businesses are not required to delete information upon request where it is necessary for the business to maintain the consumer's personal information for legitimate purposes under the enumerated exceptions.⁶⁷ Exceptions include where personal information is maintained for: recording and completing transactions, detecting security incidents or protecting against malicious, deceptive, fraudulent or other illegal activities.⁶⁸ The largest concern facing lawmakers and consumers alike now is, exceptions for deletion are overly broad and business might circumvent deletion request by abusing those exceptions.

D. Right to Opt-Out of Sale

Consumers have the right to opt-out of the sale of their personal information.⁶⁹ Businesses are mandated to have a "Do Not Sell My Personal Information" button on display to inform the consumer with the right to opt-out, and provide consumers an operative mechanism to opt out.⁷⁰ In addition, the AG's CCPA regulations specify that if a consumer makes an opt-out of sale request, the business must notify

⁶² *Id.* §§ 1798.110, 115.

⁶³ *Id.* § 1798.115.

⁶⁴ *Id.* § 1798.105.

⁶⁵ *Id.*

⁶⁶ *Id.* § 1798.105(c).

⁶⁷ *Id.* § 1798.105(d).

⁶⁸ *Id.*

⁶⁹ *Id.* § 1798.120.

⁷⁰ *Id.* § 1798.135.

2019]

Desktop Publishing Example

175

any third party that was sold the consumer's information in the past 90 days that the consumer has withdrawn their consent to sell the data.⁷¹ There is no requirement that a business should verify the consumer's identity regarding a request to opt-out of sale,⁷² which means the opt-out process is less burdensome to the consumer than to the entity.

Businesses cannot sell the personal information of minors under the age of 16 unless they have opted-in to a relevant sale.⁷³ For consumers under 13 years of age, a parent or guardian must opt-in on behalf of the child.⁷⁴ In addition, the AG's proposed regulation suggested, for a request to delete, that if a business cannot verify the identity of the requestor, the business may deny the request to delete and shall instead treat the request as opt-out of sale.⁷⁵ One immediate concern that arises from this compromise is that the word "may" gives the business great discretion to grant or deny the request. Therefore, the AG's regulation is necessary where it benefits consumers by *requiring* the business to view the request in a way that can best accommodate the consumer's intent to delete the information.⁷⁶ When deletion is not possible, requiring a business to treat the request as a request to opt-out of the sale benefits the consumer by at least preventing the further proliferation of the consumer's personal information in the marketplace.⁷⁷

E. Right to Non-Discrimination

Business cannot discriminate against a consumer because they exercised any of their rights under the CCPA.⁷⁸ Discrimination includes, but is not limited to, denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, or suggesting that the consumer will receive a different price or quality of goods or services.⁷⁹ The business, however, may charge the consumer a different price or rate, provide a different level

⁷¹ *Text of Proposed Regulation*, Art 3, § 999.315(f).

⁷² *Id.* § 999.315(h).

⁷³ *Id.* §§ 999.331-332.

⁷⁴ *Id.*

⁷⁵ *Id.* §999.313.

⁷⁶ *Initial Statement of Reason*,
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf> (last visited Oct 15, 2019).

⁷⁷ *Id.*

⁷⁸ CAL. CIV. CODE § 1798.125 (2018)

⁷⁹ CAL. CIV. CODE § 1798.125, subd. (a)(1).

or quality of goods or services, or offer financial incentives if that is reasonably related to the value provided to the business by the consumer's data.⁸⁰

COMPLIANCE AND OPERATIONAL OBSTACLES

While the California AG provided initial guidance on CCPA compliance, there are still questions unanswered and gaps unfilled. Some operational obstacles that could hinder compliance hence weaken CCPA's protection of consumer privacy are as follows:

A. The Data Mapping Challenge

Companies within the scope of the CCPA have to find ways to capture all the information they have on consumers and to track the data flow across different databases, some might be outdated. It is a significant undertaking for most companies.⁸¹ At the minimum, companies must identify where and how the personal information is stored.⁸² It involves cross-functional teams with representatives from legal, IT, compliance and key business units to adequately fulfill the task.⁸³ For smaller companies, this step alone imposes tremendous compliance and financial burden. Smaller companies simply do not have the internal compliance staffs, or massive budgets for outside counsel and consultants to fulfill the requirements.

For companies engaged with third party vendors, vendor management will be a major challenge for them. First, neither the law itself nor the AG's draft regulations provide a clear definition of what constitute a "sale". Second, the process of identifying third-party transfer, classifying the nature of the transfers, and updating relevant contractual agreements will involve substantial effort.

B. The Cost-Benefit Approach and Trade-Offs

While CCPA was supposed to regulate the privacy-invasive practices of tech giants like Google and Facebook and other data

⁸⁰ CAL. CIV. CODE § 1798.125, subd. (a)(2), (b)(1).

⁸¹ Associate General Counsel for privacy and data security at Gap shared his concern with The Wall Street Journal. See Patience Haggin, *Businesses Across the Board Scramble to Comply with California Data-Privacy Law*, WALL ST. J., (Sept. 8, 2019, 9:00 AM), <https://www.wsj.com/articles/businesses-across-the-board-scramble-to-comply-with-california-data-privacy-law-11567947602?mod=searchresults&page=1&pos=5>.

⁸² *Id.*

⁸³ *Id.*

2019]

Desktop Publishing Example

177

brokers, it overreaches to most of the businesses – many of which cannot afford the burden of compliance.⁸⁴ For example, the law will cover your neighborhood grocery store if it accepts purchases from more than 137 unique consumers per day, and 50,000-plus consumers per year, regardless of revenue.⁸⁵

The Act, together with AG’s regulation guidance, requires businesses to offer straightforward format and languages to help consumer facilitate their privacy rights, and to train all the applicable employees to get ready for compliance. This involves tremendous costs.⁸⁶ One way or another, businesses will pass along the compliance’s costs to consumers. After a risk-based assessment, businesses might conclude that cost of compliance is greater than the penalty of non-compliance and decide to scarify consumer rights of privacy over business interest. Or, to the extent the Act inhibits currently profitable practices, businesses will stop providing such services to consumers. Either way, consumers are not getting the rights the Act promised them.

C. Consumer Awareness

The CCPA’s impact is partially contingent on how easy it is for consumers to understand and exercise their rights in real time. Looking at the opt-in requirement under GDPR as an example, where consumers are often confronted by a lot of confusing “manage cookies” options or pop-up windows, most consumer will simply click “ok” to access the desired content.⁸⁷ The cookie choices impose a

⁸⁴ Eric Goldman, *The California Consumer Privacy Act Should be Condemned*, TECHNOLOGY & MARKETING BLOG, (Aug. 9, 2018), <https://blog.ericgoldman.org/archives/2018/08/the-california-consumer-privacy-act-should-be-condemned-not-celebrated-cross-post.htm>.

⁸⁵ *Id.*

⁸⁶ “On the low end, the researchers estimated that firms with fewer than 20 employees might have to pay around \$50,000 at the outset to become compliant. On the high end, firms with more than 500 employees would pay an average of \$2 million in initial costs, the researchers estimated. The \$55 billion researchers estimated companies will initially pay to become compliant is equivalent to about 1.8% of California’s Gross State Product in 2018, according to the report.” *Standardized Regulatory Impact Assessment, California Consumer Privacy Act of 2018 Regulations*, BERKELEY ECONOMIC ADVISING AND RESEARCH, (Aug, 2019) http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

⁸⁷ Greg Sterling, *CCPA Will Take Effect in About Three Months But Will Consumer Really Care?* MARKETINGLAND, (Sep. 23, 2019), <https://marketingland.com/ccpa-will-take-effect-in-about-three-months-but-will->

significant burden on consumers who don't fully understand all the cookie categories and their functions.⁸⁸ Similarly, in a post-CCPA environment, some consumers might not be sophisticated enough to understand the rights conferred to them if the platforms are providing complicated and confusing data protection choices. The enforceability hinders by consumers' willingness and ability to exercise their rights.⁸⁹

D. An Effective Compliance Program?

The CCPA requires that applicable employees within the business that handle consumer inquiries shall be aware of the provision of the law.⁹⁰ Yet no detailed guidance stating how the training should be implemented. For business with substantial direct consumer facing operations, like retail and hospitality industries, such training will be a crucial first step for CCPA compliance and for proper protection of consumer privacy rights. Additionally, neither CCPA nor the AG regulation guidance require an audit and monitor program to oversight CCPA compliance. Hence, it would be extremely difficult for consumer to check whether the business is actually fulfilling their obligations upon verifiable consumer requests.

LOOKING FORWARD

The passage of CCPA is causing a national shift in the data privacy landscape.⁹¹ Recently, 12 states have proposed consumer privacy regulations modeled after the CCPA.⁹² If passed, these state laws will impose new privacy obligations on businesses to provide consumers with substantial transparency and control over their

consumers-really-care-267790

⁸⁸ *Id.*

⁸⁹ Richard Thomas, former UK information commissioner from 2002-2009 and current global strategy advisor for Hunton & Williams' Centre for Information Policy Leadership, listed several companies that have cheekily placed conditions in their privacy notices to demonstrate that consumers simply do not read them. One example included the Mephistophelian condition of agreeing to give up one's immortal soul. See <https://iapp.org/news/a/demystifying-the-risk-based-approach/>. (last visited Oct 15, 2019).

⁹⁰ CAL. CIV. CODE § 1798.130, subd. (a)(6).

⁹¹ Focal Point Insights, *How the CCPA is Impacting State Data Protection Legislation in the US*, FOCALPOINT, (updated June 25, 2019) <https://blog.focal-point.com/how-the-ccpa-is-impacting-state-data-protection-legislation-in-the-us>

⁹² See *Id.* Hawaii, Maine, Maryland, Massachusetts, Mississippi, Nevada, New Jersey, New Mexico, New York, North Dakota, Rhode Island, and Washington are addressing consumer privacy protection.

2019]

Desktop Publishing Example

179

personal information.

On a national level, federal lawmakers are looking into the fate of the CCPA as a guide as they consider a national privacy law. This California privacy law has become a *de facto* national standard.⁹³ California businesses could benefit from having a head start on compliance if a national law goes into effect. Some members of Congress have made comments on the importance of the CCPA as a model of future federal legislation.⁹⁴ Privacy is one of the inalienable rights conferred on Californians by the state Constitution. The CCPA enumerates specific privacy rights. In giving consumers greater control over their personal information, the CCPA, operationalized by these regulations, mitigates the imbalance of knowledge and power between individuals and businesses. This benefits not only individuals, but society as a whole. The empowerment of individuals to exercise their right to privacy is particularly important for a democracy, which values and depends on the autonomy of the individuals who constitute it.

⁹³ *California Sets De Facto National Data Privacy Standard*, CORPORATE COUNSEL BUSINESS JOURNAL, (Jul. 6, 2019), <https://ccbjournal.com/articles/california-sets-de-facto-national-data-privacy-standard>.

⁹⁴ *See Thune Leads Hearing Examining Safeguards for Consumer Data Privacy*, JOHN THUNE U.S. SENATOR FOR SOUTH DAKOTA (Sep. 26, 2018), <https://www.thune.senate.gov/public/index.cfm/2018/9/thune-leads-hearing-examining-safeguards-for-consumer-data-privacy>. (“Like GDPR, the new California law—which will take effect on January 1, 2020—contains many privacy mandates and severe penalties for violators. These developments have all combined to put the issue of consumer data privacy squarely on Congress’ doorstep. The question is no longer whether we need a federal law to protect consumers’ privacy. The question is what shape that law should take.”).