Santa Clara High Technology Law Journal

Volume 37 | Issue 2 Article 3

4-3-2021

BLOCKCHAIN & CCPA

Alza Jr., Gustavo

Recommended Citation

Alza Jr., Gustavo, *BLOCKCHAIN & CCPA*, 37 SANTA CLARA HIGH TECH. L.J. 231 ().
Available at: https://digitalcommons.law.scu.edu/chtlj/vol37/iss2/3

BLOCKCHAIN & CCPA

By Gustavo Alza, Jr.[1]

Privacy laws and blockchain technology have been around for over a decade; however, each continues to evolve and adapt to new technological capabilities and realities. As users and jurisdictions have recognized an individual's rights to privacy, entrepreneurs, engineers, and businesspeople have continued to develop and enhance blockchain technology. Today, blockchain technology not only transfers value via the exchanging, creation/offering, and selling of cryptocurrencies, but has also been developed to serve national security interests, supply chain management, and a plethora of other applications. With the amount of personal information stored on these networks (where many aim to be completely "permissionless" and "decentralized"), some have written on how such may interfere with individuals' privacy rights with regards to the GDPR. Since then, the California Consumer Privacy Act ("CCPA") came into effect on January 1st, 2020. As a result, California residents now have the right to delete their data, request an accounting of data shared with third parties, correct inaccurate information, and/or request that a business cease the selling of their personal data. Given the permissionless, decentralized, and immutable nature of many blockchains, complying with the CCPA presents challenges. This article will explore how and when a blockchain may be subject to the CCPA, how to develop such (privacy by design) in order to comply with the CCPA, and demonstrate that although many see blockchain as a means for entities to escape governmental and international regulation via decentralization, recognizing and complying with user's privacy rights may not only be just, but potentially good for business/trust.

[1] Juris Doctor Candidate, Privacy Certificate Candidate, Master of Business Administration Candidate, & Finance Specialization Candidate at Santa Clara University. President and Founder of the Blockchain & Compliance Legal Society at Santa Clara University School of Law. Certified Information Privacy Professional in the United States (CIPP/US IAPP). B.S. in Economics and B.A. in Political Science from Loyola Marymount University.

CONTENTS

I. BLOCKCHAIN FUNDAMENTALS

A. Distributed Ledger Technology & Blockchain Technology

The most notorious use of blockchain technology is the Bitcoin cryptocurrency which was founded in 2008 by a Satoshi Nakamoto.[2] In order to understand the implications of such, one must first understand distributed ledger technology, blockchain technology, and cryptocurrency.

Distributed ledger technology ("DLT") constitutes a network/database with numerous nodes (computing devices), where nodes each replicate and store identical copies of the ledger, which may result in a ledger which is not maintained by a central authority.[3] This may be different than centralized databases which are controlled by centralized authorities with the power to store, maintain, update, and delete data.[4] DLT databases require a consensus of the nodes on the network rather than one confirmation by a hierarchically developed storage device (as is the case with centralized databases/ledgers).[5] Such verification of the integrity of data on a DLT typically utilizes either a proof-of-work method or a proof-of-stake method; however, regardless of the method deployed, DLTs "are less likely to be manipulated in any given case as compared to data stored on one, equally secure server."[6]

The term "blockchain" refers to a distributed ledger which deploys "a chain of blocks to provide a secure and valid distributed consensus."[7] Blockchains essentially solve the issue of trust when transacting with unknown third parties via the utilization of DLT by "raising the barriers for manipulation of stored data."[8] On blockchains, data is stored in encrypted blocks bundled with data,

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, https://bitcoin.org/bitcoin.pdf.

[3] Shaan Ray, *The Difference Between Blockchains & Distributed Ledger Technology*, TOWARDS DATA SCIENCE (Feb. 19, 2018), https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92.

[4] Douglas Malcolm*, What is a Distributed vs. Local/Centralized Databases*, GROOPE MULTIMEDIA (July 29, 2019), https://groope.io/what-is-a-distributed-vs-local-centralized-databases/.

[5] Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1371 (2018).

[6] *Id.*

[7] Ray, *supra* note 3.

[8] Zetzsche et al., *supra* note 5.

wherein the blocks serve as containers for data points stored in a particular order referred to as a "chain."[9] Given the encryption of each individually time-stamped block linked in a particular order, compromising a large blockchain network requires sophistication.[10] Blockchains typically utilize validating nodes and participating nodes.[11] Participating nodes each contain a synchronized copy of the data on the DLT. [12] On the other hand, validating nodes add data to the DLT using the proof-of-work or proof-of-stake consensus methods previously discussed.[13]

For understanding, assume that there is a DLT with one hundred nodes that store information relating to transactions. Now, imagine a centralized database that also stores the same information. If a malicious actor was to compromise one of the hundred nodes on the DLT, the remaining ninety-nine nodes would still have uncompromised data. Now, imagine that same malicious actor compromising the centralized database. Assuming that the database has not been backed up to the exact point at which the compromise has taken place, the data on the centralized database has been compromised. On the other hand, when the DLT reconciles and validates the transactions across the nodes, the majority of the nodes would reflect the uncompromised data, resulting in a consensus free from compromised data. Now, imagine a DLT with thousands or millions of nodes. In order to compromise the DLT, a malicious actor would need to "control the majority of the hash rate" (51% attack) wherein, the "attacker would have enough mining power to intentionally exclude or modify the ordering of transactions," and potentially "reverse transactions made."[14] That being said, the expense to do so will depend on the number of nodes on the DLT. Moreover, it will also depend on whether the blockchain allows users to verify transactions or institutes a permissioned blockchain.

[9] *Id.* at 1372.

[10] *Id.*

[11] *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?*, at 46, PE 634.445 (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[12] *Id.*

[13] *Id.* at 46.

[14] *What is a 51% Attack,* BINANCE ACADEMY (Nov. 2020).

B. Private Permissioned vs. Public Permissionless

Blockchains/DLTs can either be permissioned or permissionless.[15] Permissioned blockchains are similar to the hierarchical nature of centralized databases as they are "essentially private networks where data authorization depends upon the agreement of multiple predefined servers."[16] Permissioned blockchains use a governance structure which decides who can participate and validate on the blockchain network.[17] For example, Ripple, a DLT-based transaction network governs which parties can serve as validation nodes, and restricts such to "trusted parties."[18]

In addition to the aforementioned, permissioned blockchains are not necessarily transparent and may implement consensus mechanisms; however, there is "no need for consensus-based mechanisms where the entire network must agree to a change."[19]

On the other hand, permissionless blockchains are transparent, giving all users "access to all information apart from just the private keys, and this can include addresses, freedom to see transactions process by the network, and the way in which transactions are processed into blocks."[20] Bitcoin is a permissionless blockchain, which operates "on public domain software and allow[s] anyone who downloads and runs the software to participate."[21] Additionally, permissionless blockchains are typically "immutable," meaning that a blockchain ledger is "permanent, indelible, and unalterable history of transactions."[22] Permissionless blockchains will not allow data on the blockchain to be removed or modified unless allowed by some mechanism in the blockchain's underlying code.[23]

[15] Zetzsche et al., *supra* note 5, at 1372.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Toshendra Kumar Sharma, *Permissioned and Permissionless: A Comprehensive Guide*, BLOCKCHAIN COUNSEL, https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/.

[20] *Id.*

[21] Zetzsche et al., *supra* note 5, at 1372.

[22] Kevin Doubleday, *Why Blockchain Immutability Matters,* HACKERNOON (Nov. 2, 2018), https://hackernoon.com/why-blockchain-immutability-matters-8ce86603914e.

[23] Li Peng et al., *Privacy Preservation in Permissionless Blockchain: A Survey*, DIGITAL COMMUNICATIONS AND NETWORKS (June 25, 2020), https://www.sciencedirect.com/science/article/pii/S2352864819303827.

That being said, decentralized blockchains like Tezos allows the blockchain to govern "itself by establishing a true digital commonwealth."[24] Essentially, Tezos aims "to make their token holders work together to make decisions that will improve their protocol over time."[25]

C. Cryptocurrency

The term "cryptocurrency" refers to a digital asset which "uses cryptography (a form of encoding) to authenticate transactions."[26] Cryptocurrency does not necessarily utilize blockchain technology. Moreover, given a lack of a "physical presence,"[27] such cryptocurrency is "not backed by any government and is not legal tender in any jurisdiction,"[28] nor is such cryptocurrency "redeemable at most U.S. financial institutions."[29]

Cryptocurrency's value is tied to the public's perception of the currency and is usually tied to the trust of a blockchain which stores the verification data of transactions of the cryptocurrency.[30] Additionally, owners of cryptocurrency have a unique "public key" (which is recorded on the blockchain) that requires that owner's "private key" (which are kept confidential) in order to sign or transfer the cryptocurrency.[31] Given the complexity of these keys, those who use cryptocurrency usually rely on software "wallets" deployed on phones, computers, and networks.[32] Once transactions on a blockchain's ledger are recorded, such are typically immutable and un-reversable.[33]

[24] Rajarshi Mitra, *What is Tezos? The Most Updated Deep Dive*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-tezos/.

[25] *Id.*

[26] Lisa Miller, *Getting Paid in Bitcoin Attorneys Accepting Cryptocurrency as Payment Should Be Sensitive to the Fact That the Regulatory Landscape Is Likely to Change in the Near Future*, L.A. LAW., Dec. 2018, at 18–20.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Miller, *supra* note 26.

[33] *Id.*

D. Decentralized Applications

Cryptocurrency is not the only application of blockchain technology.[34] In fact, Ethereum has revolutionized the potential for applications utilizing blockchain technology.[35] Like Bitcoin, Ethereum utilizes a native cryptocurrency (Ether); however, unlike Bitcoin, "Ethereum is programmable, which means that developers can use it to build new kinds of applications."[36] These new types of applications are referred to as "decentralized applications" ("DAPPS"), which "gain the benefits of cryptocurrency and blockchain technology" as "[t]hey can be trustworthy, meaning that once they are 'uploaded' to Ethereum, they will always run as programmed."[37] Interestingly, Ethereum is decentralized, and "is maintained and improved over time by a diverse global community of contributors who work on everything from the core protocol to consumer applications."[38]

II. THE CALIFORNIA CONSUMER PRIVACY ACT

SB-1121 California Consumer Privacy Act of 2018 ("CCPA") came into effect on January 1, 2020.[39] In order to discuss the implications of the CCPA on Blockchain, one must have a fundamental understanding of the data subject to regulation and the parties regulated by the CCPA. In addition to understanding the aforementioned, consumers have "various rights with regard to personal information relating to that consumer that is held by a business."[40] This section will have two major objectives. First, this section will address the scope of the legislation, then break down each right a California resident has under the CCPA. Then this section will address potentially applicable exceptions.

[34] Jake Frankenfield, *Decentralized Applications – dApps*, INVESTOPEDIA, https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp (last updated Feb. 12, 2021).
[35] *Decentralized Applications (Dapps)*, ETHERIUM, https://ethereum.org/en/dapps/.
[36] *What is Ethereum?*, ETHEREUM, https://ethereum.org/what-is-ethereum/.
[37] *Id.*
[38] *Id.*
[39] California Consumer Privacy Act, S.B. 1121, 2018 Leg. (Cal. 2018).
[40] *Id.*

A. Definitions

1. Personal Information

An important concept to understand is the type of information to which the CCPA applies to. Unlike many other laws which regulate "personally identifiable information" ("PII"), the CCPA regulates consumers' "personal information" ("PI").[41] This distinction is important as data that falls into this category is not only such that "identifies" a user, but also includes data that "relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[42]

PI may include identifiers such as real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol Address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."[43] In addition to the aforementioned, PI also includes "characteristics of protected classifications under California or federal law," "commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies."[44] Lastly, PI includes biometric information, network activity information, geolocation data, audio, electronic, visual, thermal, olfactory or similar information, professional/employment-related information, education information, and "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[45] Simply stated, the CCPA defines PI broadly.

2. Consumer

In order to comprehend the scope of the CCPA one needs to understand that the CCPA applies to "consumers."[46] The definition for such is straight forward. According to § 1798.140(9)(g) a "consumer means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of

[41] *Id.*
[42] *Id.* at § 1798.140(o)(1).
[43] *Id.* at § 1798.140(o)(1)(A).
[44] *Id.* at § 1798.140(o)(1)(C)–(D).
[45] S.B. 1121 § 1798.140(o)(1)(E)–(K).
[46] *Id.* at § 1798.140(9)(g).

Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier."[47] Although the definition may seem narrow, "any unique identifier" is broad, and could include information not typically associated with "personally identifiable information," as discussed in the previous section.[48] In practice, this may have large implications as many businesses will likely store Consumers' PI.

3. Business

Although the definition of consumer is relatively straight forward, the definition of a "Business" is very broad as it will include any sole proprietorship or legal entity

> "that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds."[49]

The first threshold is met if a business that has "annual gross revenues in excess of twenty-five million dollars."[50] The second threshold is met if the business "buys, received for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices."[51] Although this may sound like many consumers, the fact of the matter is that a mere 137 daily visitors to a website would reach the second threshold.[52] The last threshold indicates that a business is subject to the CCPA if they derive "50 percent or more of its annual revenues from selling consumers' personal information."[53]

[47] *Id.* at

[48] Nefi Acosta, *Are IP Addresses 'Personal Information' Under CCPA?*, IAPP (Apr. 28, 2020), https://iapp.org/news/a/are-ip-addresses-personal-information-under-ccpa/

[49] S.B. 1121 § 1798.140(c).

[50] *Id.*

[51] *Id.*

[52] 50,000/356=136.99

[53] S.B. 1121 § 1798.140(c)(2).

In addition to the aforementioned, a business is "any entity that controls or is controlled by a business."[54] Control is defined as the "ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business," or "control in any manner over the election of a majority of directors," or "the power to exercise a controlling influence over the management of a company," or an entity that "shares common branding with the business" (where "Common branding" means "a shared name, service mark or trademark").[55]

In practice, this means that a non-profit or other entity could potentially be subject to the CCPA if it is "controlled by a business" or "shares common branding with the business."[56]

4. Business Purpose

The term "business purpose" is sprinkled throughout the CCPA and understanding its meaning will be important in further analysis.[57] Section 9 of the CCPA amends § 1798.140(d) of the Civil Code to define "[b]usiness purpose" to mean use of PI "for the business's or a service provider's operational purposes, or notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed" or "for another operational purpose that is compatible with the context in which the personal information was collected."[58]

In addition to the aforementioned definition of business purpose, the CCPA further clarifies the term by listing seven business purposes;[59] however, for the purposes of this article, four purposes will be covered.

Section 1798.140(d)(1) relates to auditing interactions with consumers and transactions, "including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of

[54] *Id.*

[55] *Id.*

[56] Nate Garhart, *Nonprofits and the California Consumer Privacy Act*, FARELLA BRAUN + MARTEL (June 20, 2019), https://www.fbm.com/publications/nonprofits-and-the-california-consumer-privacy-act/.

[57] *California Consumer Privacy Act of 2018*, IAPP: RESOURCECENTER, https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/.

[58] S.B. 1121 § 1798.140(d).

[59] *Id.*

ad impressions, and auditing compliance with this specification and other standards."[60]

Section 1798.140(d)(2) relates to "[d]etecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity."[61]

Section 1798.140(d)(5) is also applicable as it relates to performing "services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider."[62]

Section 1798.140(d)(7) relates to "activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, or manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business."[63]

The application of these business purposes will be discussed in the following analysis.

5. Commercial Purpose

The CCPA draws a distinction between a business purpose and a "commercial purpose."[64] A "commercial purpose" is anything that advances a "person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction."[65] Commercial purposes do not include purposes related to engaging in speech that state or federal courts recognize as "noncommercial speech, including political speech and journalism."[66]

6. Sell, Selling, Sale, or Sold

A business sells data when it sells, rents, releases, discloses, disseminates, makes available, transfers, or otherwise communicates

[60] *Id.* at § 1798.140(d)(1).
[61] *Id.* at § 1798.140(d)(2).
[62] *Id.* at § 1798.140(d)(5).
[63] *Id.* at § 1798.140(d)(7).
[64] S.B. 1121 § 1798.140.
[65] *Id.* at § 1798.140(f).
[66] *Id.*

orally, in writing, or by electronic or other means, "a consumer's personal information by the business to another business or third party for monetary or other valuable consideration."[67] Where the Supreme Court of California has accepted consideration as the bargained-for exchange concept from the second Restatement of Contracts in *Jara v. Suprema Meats, Inc.*[68] where "the key question is whether the exchange [is] 'motivated' or 'induced' the other party's promise or performance."[69]

B. Consumer Rights

The CCPA grants a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to notice, the right to access, the right to opt-out, the right to request deletion, and the right to equal services and prices. [70]

1. Right to Notice

The CCPA grants consumers the right to conspicuous "[n]otice at collection" which means that notice must be given by a business to a consumer "at or before the point at which a business collects personal information."[71] Moreover, California's attorney general has clarified that the CCPA requires that every business "provide a privacy policy in accordance with the CCPA and these regulations."[72] In addition, if a business sells personal information, then it must "provide notice of the right to opt-out in accordance with the CCPA and these regulations."[73] Lastly, if businesses offer financial incentives or price or service differences must "provide a notice of financial incentive in accordance with the CCPA."[74] If a business does not provide notice at or before the point of collection

[67] *Id.*

[68] Alexander Scott et al., *'Sale' Under CCPA May Not be as Scary as You Think,* IAPP (Oct. 29, 2019), https://iapp.org/news/a/sale-under-the-ccpa-may-not-be-as-scary-as-you-think/.

[69] *Id.*

[70] California Consumer Privacy Act Regulations Proposed Text of Regulations, 2020 Leg. § 999.301(l) (Cal. 2020), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf?.

[71] *Id.*

[72] *Id.* at § 999.304(a).

[73] *Id.* at § 999.304(c).

[74] *Id.* at § 999.304(d).

then a business "shall not collect personal information from the consumer."[75]

2. Right to Access

The CCPA mandates that if a business receives a "verifiable consumer request" to access personal information, then the business "shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section."[76] The CCPA also requires that the information be "delivered by mail or electronically, if provided electronically, the information shall be in a portable and, to the extent technologically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance."[77] A business is not required to honor more than two data access request made in a 12-month period.[78] The specific information that is required to be disclosed by businesses includes "[t]he categories of personal information it has collected about that consumer,"[79] "[t]he categories of sources from which the personal information is collected,"[80] "[t]he business or commercial purpose for collecting or selling personal information,"[81] "[t]he categories of third parties with whom the business shares personal information,"[82] and "[t]he specific pieces of personal information the business has collected about that consumer."[83]

In addition to the aforementioned, if a business sells PI, then a business must disclose "[t]he category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact,"[84] "[t]he category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact."[85]

[75] *Id.* at § 999.305(a)(7).

[76] California Consumer Privacy Act, S.B. 1121, 2018 Leg. § 1798.100(d) (Cal. 2018).

[77] *Id.*

[78] *Id.*

[79] *Id.* at § 1798.100(c)(1).

[80] *Id.* at § 1798.100(c)(2).

[81] *Id.* at § 1798.100(c)(3).

[82] California Consumer Privacy Act, S.B. 1121, 2018 Leg. § 1798.100(c)(4) (Cal. 2018).

[83] *Id.* at § 1798.100(c)(5).

[84] *Id.* at § 1798.115(c)(1).

[85] *Id.* at § 1798.115(c)(2).

3. Right to Opt-Out

Section 5 of the CCPA amends Section 1798.120 of the Civil Code codifies a consumer's right to opt-out when it states that "A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[86] In addition, a business that has the PI of consumers younger than 16 may not sell such unless they have received affirmative authorization to sell such from the consumer's parent or guardian.[87]

4. Right to Request Deletion

Like the GDPR's right to erasure, the CCPA grants consumers "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[88] Upon a "verifiable consumer request" to delete a consumer's PI, a business "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records."[89]

That being said, there are circumstances in which a business "shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information."[90] First, a business does not need to comply with a deletion request so that the business can "[c]omplete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer."[91] Second, a business does not need to comply with a request for deletion if the data is required to "[d]etect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."[92] Third, a business does not need to comply with a consumer's request to delete

[86] *Id.* at § 1798.120(a).
[87] *Id.* at § 1798.120(c).
[88] California Consumer Privacy Act, S.B. 1121, 2018 Leg. § 1798.105(a) (Cal. 2018).
[89] *Id.* at § 1798.105(c).
[90] *Id.* at § 1798.105(d).
[91] *Id.* at § 1798.105(d)(1).
[92] *Id.* at § 1798.105(d)(2).

personal information if such is used to "[d]ebug to identify and repair errors that impair existing intended functionality."[93] Fourth, businesses are not required to comply with a consumer's request to delete personal data where the personal data constitutes an "[e]xercise [of] free speech, ensure[s] the right of another consumer to exercise his or her right of free speech, or exercise another right provided by law."[94] Fifth, a business is not required to comply with a consumer's request for deletion in order to "[c]omply with the California Electronic Communications Privacy Act."[95] The sixth enumerated exemption to complying with a consumer's deletion request is where the business "[e]ngage[s] in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws" if "the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent."[96] The seventh enumerated scenario where a business is not required to comply with a consumer's request for deletion is "[t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[97] The eighth and ninth enumerated scenarios where a business does not need to comply with a consumer's request to delete a consumer's personal information are "[t]o comply with a legal obligation,"[98] or to "[o]therwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."[99]

5. Right to Equal Services and Prices

The last right relates to a business not discriminating against a consumer because they "exercised any of the consumer's rights."[100] Accordingly, business may not deny goods or service to consumers, charge different prices for goods or services, provide different levels

[93] *Id.* at § 1798.105(d)(3).

[94] California Consumer Privacy Act, S.B. 1121, 2018 Leg. § 1798.105(d)(4) (Cal. 2018).

[95] *Id.* at § 1798.105(d)(5).

[96] *Id.* at § 1798.105(d)(6).

[97] *Id.* at § 1798.105(d)(7).

[98] *Id.* at § 1798.105(d)(8).

[99] *Id.* at § 1798.105(d)(9).

[100] California Consumer Privacy Act, S.B. 1121, 2018 Leg. § 1798.125(1) (Cal. 2018).

of quality of goods or services, suggest consumers will receive different prices or rates for goods or services.[101]

III. The Extensive Territorial Scope of CCPA

A. Broad Applicability to "Business" Globally

Although the CCPA applies to certain organizations that conduct business in California, and collect "consumers" "personal information," the fact of the matter is that there are various forms of blockchain and crypto currency organizations which will impact the California Attorney General's ability to enforce the CCPA, as well as challenges for blockchain organizations that qualify as businesses and have yet to be permissionless and therefore centralized.[102]

Some cryptocurrency/blockchain organizations are not legal entities, permissionless, and have no ultimately responsible party. Meaning, that it would be difficult to enforce the CCPA in such an instance. That being said, corporations and non-profits who ultimately control, permission, or own a blockchain create a path to compliance with the CCPA as such could potentially be a "business" if they do business in California.

Moreover, for centralized exchanges of Cryptocurrency, given the numerous compliance obligations (including FinCEN, AML, KYC) which come as a result of value transmission, compliance with CCPA may require more sophistication.

B. Significance of "Consumer"

With a population of 39 million,[103] it is likely that many blockchain and crypto currency organizations will collect, store, process, and sell Californian consumer personal information.

This means that "businesses" will need to comply with consumer requests for deletion of data so long as there is no provision excusing such in the CCPA or another California or Federal law requiring the retention of aforementioned personal information.

[101] *Id.* § 1798.125(1)(a)–(d).

[102] *See supra* Section II.

[103] United States Census Bureau, QuickFacts California, https://www.census.gov/quickfacts/CA (last visited Mar. 27, 2021).

IV. Allocation of Responsibility

A. Businesses

"Businesses" will ultimately be responsible. The issue here is whether the blockchain/cryptocurrency organization or organization utilizing blockchain technology is business. For example, although Bitcoin will probably not qualify as a business as it is not "[a] sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners."[104]

That being said, businesses like Coinbase,[105] Robinhood,[106] Kraken[107] and Gemini,[108] which are centralized exchanges of cryptocurrency,[109] will have to not only comply with the CCPA but will also need to consider financial regulations given their money service business status.[110] For example, the Bank Secrecy Act, "requires Coinbase to verify customer identities, maintain records of currency transactions for up to 5 years, and report certain transactions."[111] Moreover, the Patriot Act, "requires Coinbase to designate a compliance officer to ensure compliance with all applicable laws, create procedures and controls to ensure compliance, conduct training, and periodically review the compliance program."[112] Moreover, if Coinbase was to receive a proper national security letter,

[104] Lydia F de la Torre, *What is a 'Business' Under CCPA?*, MEDIUM (Dec. 10, 2018), https://medium.com/golden-data/what-is-a-business-under-ccpa-350f7d20a74.

[105] COINBASE, https://www.coinbase.com.

[106] ROBINHOOD, https://robinhood.com/us/en/?utm_source=google&utm_campaign=8140492015&utm_content=84157058397&utm_term=397665157904__%2Brobinhood__b&gclid=EAIaIQobChMIkLrb18SO6QIVkPhkCh305Ad4EAAYASAAEgJRr_D_BwE.

[107] KRAKEN, https://www.kraken.com.

[108] GEMINI, https://gemini.com.

[109] Nathan Reiff, *What Are Centralized Cryptocurrency Exchanges?*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/.

[110] FINANCIAL CRIMES ENFORCEMENT NETWORK, US TREASURY, FINCEN EXTENDS COMMENT PERIOD FOR RULE AIMED AT CLOSING ANTI-MONEY LAUNDERING REGULATORY GAPS FOR CERTAIN CONVERTIBLE VIRTUAL CURRENCY AND DIGITAL ASSET TRANSACTIONS (Jan. 14, 2021), https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering.

[111] *Is Coinbase Regulated?*, COINBASE: LEGAL, https://www.coinbase.com/legal/faq.

[112] *Id.*

it would be obligated to tender any requested information.[113] Exchanges are in an interesting position because they are legally obligated to retain personal information.[114] Thus, "most, if not all, financial institutions will need to comply with applicable notice, disclosure, opt-out, and other obligations under GLBA/CalFIPA and FCRA, as well as under the CCPA with respect to different types of PI that they collect and process."[115]

B. Governments

The CCPA generally vests enforcement in "the Attorney General, but also provides for a private right of action."[116] Moreover, the Attorney General is empowered with power to assess civil penalties to ensure compliance wherein, "the civil penalty to be assessed in an Attorney General action in this context to not more than $2,500 per violation or $7,500 per intentional violation and would specify that an injunction is also available as remedy."[117]

Moreover, the CCPA generally exempts the Government from any and all obligations required of businesses. Meaning, the CCPA does not restrict the Government's collection, use, transmission, "selling" of California residents.[118] For example, the government could possibly utilize blockchain technology to require permissioned nodes to reach a consensus before altering critical assets.[119] In addition, maybe the best way to record property titles is

[113] Aravind Swaminathan & Harry Clark, *What Happens When My Company Receives a National Security Letter? A Primer.*, TRUST ANCHOR: CYBER, PRIVACY & INNOVATION – ORRICK BLOG (Oct. 13, 2016), https://blogs.orrick.com/trustanchor/2016/10/13/what-happens-when-my-company-receives-a-national-security-letter-a-primer/.

[114] *Know Your Customer: Quick Reference Guide*, PWC (Jan. 2016), https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-2016.pdf.

[115] Glenn A Brown et al., Squire Patton Boggs, *I'm a Financial Institution – What do I Need to do Under the CCPA?*, NAT'L. L. REV., Nov. 5, 2019, https://www.natlawreview.com/article/i-m-financial-institution-what-do-i-need-to-do-under-ccpa.

[116] California Consumer Privacy Act, S.B. 1121(3) (Cal. 2018).

[117] *Id.*

[118] Mark Lyon et al., Gibson Dunn & Crutcher LLP, *Should Consumer Data Privacy Laws Apply to the Gov't?*, LAW360 (June 17, 2019), https://www.gibsondunn.com/wp-content/uploads/2019/06/Lyon-Gaedt-Sheckter-Rangarajan-Should-Consumer-Data-Privacy-Laws-Apply-To-The-Govt-Law360-06-07-2019.pdf.

[119] Christian Cachin et al., *Blockchain, Cryptography, and Consensus*, IBM RESEARCH – ZURICH (June 2017), https://crypto.unibe.ch/talks/20170622-blockchain-ice.pdf.

to put such on an immutable blockchain ledger.[120] Or maybe, the Government could create a public blockchain transportation network which would ensure the safety of passengers be requiring network consensus before altering the path of an autonomous vehicle.[121] Who knows what blockchain applications can be created and utilized by the government. The fact of the matter is that the government is not restricted.

The government is not given any additional obligations outside of enforcement. Meaning, that the Government does not qualify as a "business" and is under no obligation to comply with Californian requests for access, deletion, or opting out of sales. That being said, private "businesses" may contract with the government and be subject to the CCPA.

C. Nonprofits

As discussed above, the CCPA does not apply to non-profits so long as they are not owned by a business or share common branding with such. Therefore, if an organization develops or implements blockchain or cryptocurrency technology as a non-profit (not owned or controlled by a "business" or sharing common branding with a "business), then it seems unlikely that the California Attorney General would be able to bring claims against the non-profit as such would be outside the jurisdiction of the CCPA.

That being said, this may get complicated as a business could hypothetically establish an independent nonprofit association[122] which is neither controlled nor owned by the establishing business. An example of such would the Libra, wherein, Facebook established the Libra association.[123]

This is a matter which will possibly be addressed by either the Attorney General of California or the courts. That being said, if this is not addressed, it seems likely that organizations may

[120] *Here's What a Blockchain Property Deed Looks Like*, GOVERNMENT TECHNOLOGY (April 16, 2018), https://www.govtech.com/biz/Heres-What-a-Blockchain-Property-Deed-Looks-Like.html.

[121] Madhusudan Singh & Shiho Kim, *Branch Based Blockchain Technology in Intelligent Vehicle*, COMPUTER NETWORKS 145 (2018), https://www-sciencedirect-com.libproxy.scu.edu/science/article/abs/pii/S1389128618308399?via%3Dihub.

[122] DIEM, https://libra.org/en-US/association/.

[123] Nick Statt, *Facebook is Shifting its Libra Cryptocurrency Plans After Intense Regulatory Pressure*, THE VERGE (Mar. 3, 2020), https://www.theverge.com/2020/3/3/21163658/facebook-libra-cryptocurrency-token-ditching-plans-calibra-wallet-delay.

circumvent compliance obligations by the creation and operation of a non-profit entity.[124]

D. Consumers

Ultimately, the CCPA puts much of the responsibility on the shoulders of consumers. In order for rights to erasure/deletion, correction, or access to be implemented, consumers must exercise such. That being said, consumers will likely play a significant role with respect to exercising and reporting when they believe violations of the CCPA have been effectuated.

E. Developers

Developers will not be responsible for compliance with the CCPA simply because they are "developers." If a developer hypothetically develops a new blockchain technology which collects and transmits personal information, where such is not conducted as business, or owned or operated for the benefit of any shareholder, then it is possible that such does not qualify as a business.

F. Miners & Nodes

As previously stated, miners and nodes may be required to comply with the CCPA if they qualify as a business and meet CCPA requirements as previously stated.[125]

V. COMPLYING WITH CONSUMER REQUESTS IN BLOCKCHAIN

Complying with consumer requests will be different amongst the various organizational and technological structures. The distinction between permissioned and permissionless may seem to be significant in this regard.[126]

[124] Bryan Cave Leighton Paisner, *Privacy FAQs: Does the CCPA Apply to Non-profits*, JDSUPRA (Apr. 10, 2019), https://www.jdsupra.com/legalnews/privacy-faqs-does-the-ccpa-apply-to-non-95070/.

[125] *Reconciling Blockchain Technology with California Consumer Privacy Act*, COINTELEGRAPH (Aug. 17, 2019), https://cointelegraph.com/news/reconciling-blockchain-technology-with-california-consumer-privacy-act.

[126] Louis Bruno et al., *The Data Privacy Block in the Chain: Blockchains and Immutability*, EISNERAMPER (June 4, 2019), https://www.eisneramper.com/blockchain-emerge-te-blog-0619/.

A. Permissioned Blockchains

Businesses that control/own blockchain networks will be required to implement technologies to comply with the CCPA.[127] For starters, they can permission control of the access to personal information.[128] The technology would either require some automated system (capable of verification, retrieving PI, modifying PI, deleting PI, updating the consensus of the blockchain network, and the ability to adjust to rapidly changing privacy laws at local, state and federal levels[129]) to filter out personal information,[130] or require someone to comply with consumers right to notice, right to request deletion, right to access, and right to opt-out of sales.

1. Right to Request Deletion

The right to request deletion will create problems for blockchains with collect, store, or sell consumer personal information. As "the risk remains that data owners cannot edit or delete the records once they are on the blockchain."[131] Therefore, it may be a good idea to develop blockchains in a way where a business owns all the nodes and therefore can alter the consensus, or to implement blockchain technology in a way where personal information is not collected.[132] That being said, the definition of personal statement is quite broad, so developing a solution to comply with the right to request deletion seems important.

On the other hand, if the reason why a transaction remains recorded on a blockchain is so that it can prevent a fraudulent transaction and be used retroactively to verify such (possibly by the IRS[133]), then it may be the case that the storage of aforementioned data does not require the business to comply with the verifiable

[127] *GDPR, CCPA, Blockchain and Renewable Energy: Policy Lagging Behind Technology*, NAT'L L. REV., Feb. 1, 2019, https://www.natlawreview.com/article/gdpr-ccpa-blockchain-and-renewable-energy-policy-lagging-behind-technology.

[128] Bruno et al., *supra* note 126.

[129] JESSICA SANTOS, KANTER HEALTH, KEEPING UP WITH FAST-CHANGING INTERNATIONAL PRIVACY LEGISLATION (Jan. 2019), https://iapp.org/resources/article/keeping-up-with-fast-changing-international-privacy-legislation/.

[130] Bruno et al., *supra* note 126.

[131] *Id.*

[132] *Id.*

[133] Andrew Perlin, *Does Coinbase Report to the IRS?*, TOKENTAX (Feb. 24, 2021), https://tokentax.co/blog/does-coinbase-report-to-the-irs/.

consumer request for deletion as it would be one of various exemptions.[134]

B. Permissionless Blockchains

Complying with the CCPA for permissionless, decentralized blockchains will be a challenge, as it is not always evident that there is a business, let alone anyone with the ability to actually edit the immutable data on the ledger.[135] That being said, "[p]ublic permissionless blockchains reflect the technology's original notions and benefits of permitting any individual to access, view, and submit transactions with minimal data governance. Organizations must balance these benefits with their needs to follow consistent data privacy practices and comply with applicable laws and regulations."[136]

If it turns out that a business develops and deploys a permissionless, public, decentralized, blockchain which stores and transmits the personal information of consumers, then it is likely that such will be required to comply with the CCPA and be incapable of doing so as it would be impossible to delete the personal information of a consumer.[137]

The simplest way to comply with the CCPA for a business operating a permissionless blockchain is to not store personal information, and instead focus on other business areas like supply chain management, or sectors which have existing privacy laws that preempt the CCPA.[138]

VI. RECOMMENDATIONS AND WEIGHING OF OPTIONS

A. Businesses

Business's all over the world have begun to implement blockchain technology.[139] That being said, businesses should invest in

[134] *Applying the 9 CCPA Exemptions to Deletion Requests*, CLARIP, https://www.clarip.com/data-privacy/ccpa-erasure-exemptions/ (last visited Mar. 27, 2021).

[135] PRITESH SHAH ET AL., DAVIS POLK & WARDWELL LLP, BLOCKCHAIN TECHNOLOGY: DATA PRIVACY ISSUES AND POTENTIAL MITIGATION STRATEGIES, https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf.

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] Gwyneth Iredale, *List of Top 50 Companies Using Blockchain Technology*, 101 BLOCKCHAINS (Dec. 26, 2020),

blockchain if such provides utility or a competitive advantage.[140] However, businesses need to consider privacy by design as such is developed, deployed, and adapted.[141] This way, businesses can accommodate CCPA requirements (if applicable and not pre-empted or unconstitutional[142]).

B. Trust

Blockchain is a system of trust.[143] Value is derived by blockchains' ability to store truth, thereby creating a sense of security.[144] According to the MIT Technology Review, "[t]he crypto bubble, like the dot-com bubble, is creating the infrastructure that will enable the technologies of the future to be built. But there's also a key difference. This time, the money being raised isn't underwriting physical infrastructure but social infrastructure."[145] It is this social infrastructure that will disrupt and enhance business, and in order for such to work, consumers need to trust businesses, and businesses need to comply. If businesses do not comply, then there will likely be a reduction in trust and therefore a reduction in value.

https://101blockchains.com/companies-using-blockchain-technology/.

[140] Brant Carson et al., *Blockchain Beyond the Hype: What is the Strategic Business Value?*, McKinsey Digital (June 19, 2018), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

[141] Ann Cavoukian, Privacy by Design, The 7 Foundational Principals: Implementation and Mapping of Fair Information Practices, IAPP (Jan. 2011), https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/.

[142] Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional*, Technology & Marketing Law Blog (July 9, 2018), https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm.

[143] Esther Shein, *How Blockchain Changes the Nature of Trust*, The Linux Foundation (Jan. 22, 2019), https://www.linuxfoundation.org/blog/2019/01/how-blockchain-changes-the-nature-of-trust/.

[144] *Id.*

[145] Michael J. Casey & Paul Vigna, *In Blockchain We Trust*, MIT Tech. Rev. (Apr. 9, 2018), https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/.

CONCLUSION

The CCPA does not outlaw Blockchain technology. Nor does it make illegal to buy, sell, and trade cryptocurrency. Instead, businesses can implement, develop, and adapt blockchain technology to innovate. However, in order to do so, it seems prudent to develop such in a permissioned (where responsibility and specific roles can be assigned) manner.[146]

Moreover, as the CCPA has a private right of action for breaches, a Blockchain's ability to comply with the CCPA will also affect its ability to build trust with consumers.[147] Consumers want to store their data on secure places; however, they may be sensitive with respect to their personal information and blockchains that can avoid civil penalties and private right of actions[148] will likely save plenty of money and get additional customers. Therefore, complying with the CCPA is good for business.

[146] SHAH ET AL., *supra* note 135.

[147] Rob Eleveld, *Embracing GDPR And CCPA To Build Consumer Trust*, FORBES: TECHNOLOGY COUNCIL (Nov. 15, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/11/15/embracing-gdpr-and-ccpa-to-build-consumer-trust/#21f0701e7951.

[148] Ian Ballon & Rebekah Guyon, *Anticipating the Flood of Cybersecurity Litigation Under the CCPA – What to Do About It*, LAW.COM (Jan. 25, 2019), https://www.law.com/therecorder/2019/01/25/anticipating-the-flood-of-cybersecurity-litigation-under-the-ccpa-what-to-do-about-it/.