California Blockchain Working Group

Blockchain and Privacy
Jason Albert and Radhika Iyengar

I. California Context

California is a leader on privacy protections, having adopted the nation's first comprehensive privacy law, the California Consumer Privacy Act (CCPA) (Cal. Civil Code § 1798.100 et seq.). In addition, there likely will be a follow-on ballot initiative, the California Privacy and Enforcement Rights Act, this year.[1] In addition to these landmark measures, California businesses are subject to a number of other privacy laws, depending on the type of data they process and where they do business. California businesses that collect data from European Union residents are subject to the EU General Data Protection Regulation (GDPR).[2] Those in the healthcare space must comply with the Health Insurance Portability and Accountability Act (HIPAA).[3] Educational institutions must comply with the Family Educational Rights and Privacy Act (FERPA).[4] Financial institutions are subject to the requirements of the Gramm-Leach-Bliley Act (GLBA).[5]

Thus, as the State of California and California businesses implement blockchain, they must do so in compliance with potentially several privacy laws—as well as in cognizance of potential future privacy legislation at the Federal level, where several bills are pending. While the privacy laws above vary considerably in their specifics, most of them provide some combination of the rights embodied in Fair Information Principles developed by the Organisation for Economic Co-operation and Development (OECD) in 1980 (a revised version of these can be found in the OECD Privacy Framework).[6] These Principles, derived from work done at the dawn of the age of computing by the U.S. Department of Health, Education, and Welfare in 1973, define the framework of modern privacy regulation.[7]

II. Literature Review

Quite a bit has been written on blockchain and privacy. With respect to the ability of blockchains to comply with GDPR, the two main reports are the EU Blockchain Observatory's report Blockchain and the GDPR[8] and the French Data Protection Authority's (CNIL) report Solutions for a Responsible Use of the

[1] California Privacy Rights and Enforcement Act of 2020, as filed with the California Attorney General's office on November 4, 1999, available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.
[2] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 4.5.2016, p. 1).
[3] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-91, Title II.
[4] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.
[5] Financial Services Modernization Act of 1999, Pub. L. 106-102, 15 U.S.C. §§ 6801-6809.
[6] Organisation for Economic Co-operation and Development, The OECD Privacy Framework, 2013, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[7] Jason Albert, "U.S. Privacy Law: A Short History," (June 28, 2018), available at https://www.linkedin.com/pulse/us-privacy-law-short-history-jason-albert/.
[8] Blockchain and the GDPR, European Union Blockchain Observatory and Forum (October 16, 2018), available at https://www.eublockchainforum.eu/reports.

Blockchain in the Context of Personal Data.[9] Important critiques of the state of privacy compliance of blockchain solutions include Elizabeth Renieris's post Forget Erasure: Why Blockchain is Really Incompatible with the GDPR.[10]

III. Blockchain Compliance with Privacy Laws

Most of the privacy rights embodied in the OECD Fair Information Principles and the various laws pose no greater difficulty for blockchain solutions than any other technology. For example, implementers of blockchain solutions must provide notice to individuals of what data they are collecting and the purposes for which the data will be used, must have a legitimate purpose for collecting and processing the data, not use the data for other purposes aside from those specified without consent, and must implement technical and organizational measures to protect the security of the personal data. In all these cases, blockchain either doesn't impede compliance or, as in the case of security, it offers tools that can make compliance easier.

However, that doesn't mean that these requirements can be ignored. As Elizabeth Renieris notes in connection with a permissible basis for collecting and processing personal data, "Most existing projects rely on "consent" but do not effectively address the mechanism for obtaining adequate informed consent or its revocable nature." She goes on to suggest that it might be difficult to rely on GDPR's "legitimate interests" test given the automated nature of most blockchains, but that is probably overstating the case: many non-blockchain uses of personal data rely on the legitimate interests of the controller that aren't outweighed by the rights of the individual without engaging in a person-by-person balancing test.

She further suggests that replication of the data on nodes may lack a legitimate purpose, unless there is a need for the data to be replicated across a blockchain network. She also argues that data replication runs afoul of data minimization requirements—that is, only the minimum data needed for a purpose for which it is processed be used. But fundamentally blockchain operates as a distributed ledger, and the distributed nature of that ledger provides enhanced security (by making the ledger more difficult to compromise) and enabling it to operate without a single master entity. These benefits should suffice to meet the "permissible purpose" and "data minimization" tests—for data replication is essential to realizing the benefits of application of blockchain in these uses.

A. Right of Rectification and Deletion

Most concern about the ability to build a privacy-compliant blockchain solution relates to the rights of rectification and deletion. Under most privacy laws, individuals have the right to have inaccurate data about them corrected, and to have it deleted when no longer needed for the purpose for which it was

9 Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, Commission nationale de l'informatique et des libertés (November 6, 2018), available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

10 Elizabeth M. Reneiris, "Forget erasure: why blockchain is really incompatible with the GDPR" (September 23, 2019), available at https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-really-incompatible-with-the-gdpr.

collected. In addition, there is an independent obligation on data controllers to delete data when it is no longer needed for the purpose for which it was collected. However, one of the features of blockchain is there immutability—every transaction is tied to the preceding transaction cryptographically in a way that any subsequent alteration is detectable. This means that personal data, once written to a blockchain, remains there permanently.

Several commentators have suggested that this means blockchain is incompatible with laws such as GDPR that provide rights of rectification and deletion. However, it is possible to comply with GDPR's right to be forgotten, even though data stored on the blockchain is immutable, via several means. First, the recipient can delete his or her private key, breaking the association with the public key. Second, the data to which the public key relates (e.g., the credential) can be deleted, such that the public key serves no purpose. Indeed, it might be possible to hash or encrypt that data rather than deleting it.

The CNIL, the French data protection commissioner's office, has published a helpful paper on blockchain and privacy issues titled Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. Fundamentally, blockchains are used to store public keys that identify individuals, but these can effectively be rendered anonymous by the individual by deleting his/her private key, or via other measures

As the CNIL guidance states, "…*blockchain can contain two main categories of personal data*: *Identifiers of Participants* and Miners [and Additional or "Payload" Data]. *Each participant has an identifier, called a public key*, consisting of a series of alphanumeric characters that seem random. This public key refers to a private key that is only known by one person…."

Guidance thus far recognizes that it is not technically possible to "delete" information stored on the blockchain. Although definitive guidance would be helpful, alternative measures which obfuscate the information on the blockchain likely are "similar to effective erasure of data" according to the CNIL.

- **Deletion of the Private Key.** The CNIL also stated that the deletion of the private key would make it impossible to prove what payload data had been associated with the public key and as such "would no longer pose a risk to confidentiality." The self-help approach where the user has control over their information through a portal or other technology is also supported by regulators.

- **Deletion of Underlying Data.** Presumably, deletion of all the data on the centralized server that is linked to by the blockchain (so that the public key is merely a number without purpose) would satisfy the right to be forgotten.

- **Hashing or Encrypting Payload Data.** While it does not go into specifics, the CNIL acknowledges that proper hashing or encryption techniques of payload data would be an acceptable method of erasure for blockchain technology.

- **Other Options.** Additionally, over time, there may evolve approaches that are also recognized as acceptable, but were not mentioned in the guidance (e.g., scrambling payload data, multiple

public keys corresponding to specific personal data (like a new metadata approach) and other approaches.

B. Controller-Processor Distinction

1. Permissioned Blockchains

Beyond rectification and deletion, there are other privacy-related questions that have to be answered for blockchains. For example, many privacy laws distinguish between data controllers—those who determine the purposes and means of processing personal data—and data processors—those who process data on behalf of and pursuant to the instructions of a data controller.

In general, for a permissioned blockchain, the controller-processor issue can be resolved via the governing documents. In general, where a consortium operates the blockchain, it does so to provide a service to the consortium members. Thus, each of them should be the controller of the personal data they write to the blockchain, with the consortium acting as a data processor. This is consistent with guidance issued by the CNIL. As consortium members will use the blockchain for their own purposes, each will be a controller. However, if they write data to the blockchain for a common purpose, they could be considered joint controllers. It is possible for companies writing to the blockchain to designate a single entity to be the controller, per the CNIL guidance, if that entity makes decisions for the group. To achieve this controller-processor distinction, in most cases the consortium should be a separate legal entity. If it isn't, then fundamentally every consortium member is a processor for every other consortium member—or they are joint controllers (see above).

As the consortium will be a data processor, it will need to enter into data processing agreements with each controller that complies with the requirements of Article 28 of GDPR. These terms could be incorporated into the consortium agreement itself, as the consortium members will be the ones using the blockchain. Alternatively, each time a consortium member wanted to use the blockchain as part of a service, it could enter into a data processing agreement with the consortium. Either way, the relevant agreement will need to specify that the consortium member is the controller of personal data written to the blockchain and include instructions from that member to the consortium as to how that data should be processed, in addition to the other required terms in Article 28 of GDPR.

2. Permissionless Blockchains

For permissionless or decentralized ledgers, the question of who is a controller poses more of an issue. As Renieris states, "Many blockchain or ledger-based projects argue that they are too "decentralized" to identify data controller(s) or take responsibility for giving effect to data subject rights." That won't work from a privacy compliance perspective, because it means that anyone operating part of the ledger—such as a node—may then be considered a co-controller, liable for all aspects of compliance.

Where good data privacy hygiene is observed, this shouldn't be an insurmountable issue. For many applications, the only personal data that needs to be written to the blockchain is a Digital Identity

Document (DID), and the tie between that DID and an individual can be severed after the fact by various techniques (including simply having the individual destroy his or her private key). But on a permissionless blockchain, one cannot foreclose that someone may write additional personal data to the blockchain, and that the individual whose data is written there may have rights—whether under CCPA, GDPR, or another privacy law—to have that data deleted or to prevent it from being disclosed to others.

In the case of CCPA, which applies to businesses, a business that chooses to write personal data in plain text to the blockchain will likely be in a position where it is unable to comply with the Act. As it isn't clear that a node operator falls under the Act, as it may not qualify as a business or a service provider, the mere writing of personal information to a permissionless blockchain would not necessarily put that blockchain in violation of CCPA. However, it is likely a different situation with respect to GDPR. There, the data protection rules apply to any entity that has data. In the absence of a permissioned system, where there is a data processing contract between the entity writing to the blockchain and each node operator, node operators are likely co-controllers, and responsible for complying with the privacy rights of individuals whose data is written to the blockchain. This clearly is the implication of the CNIL guidance.

Although there are successful decentralized ledgers—Bitcoin itself and Ethereum to name two—most commercial applications of blockchain appear to use permissioned ledgers, which helps address responsibility and accountability for compliance.

C. Data Transfers

Because the blockchain will consist of several nodes located around the world, it will be important that the EU's standard contractual clauses (SCCs)—specifically, the controller to processor clauses—be part of the consortium agreement.[11] That way, when the consortium members operate nodes and data written to the blockchain is immediately replicated around the world on those nodes, it will be covered from a data transfer perspective. Likewise, any agreement between a consortium member and the consortium to write data to the blockchain will also need to include the SCCs.

IV. Blockchain as a Tool to Enhance Privacy

The important focus on the ability of blockchain solutions to comply with privacy laws shouldn't take away from the fact that blockchain can help enhance privacy in many situations by enabling fine-grained control on access to personal data, along with strong security protections. In particular, blockchain-based digital identity solutions enable individuals to share only those aspects of their identity they wish to with others, and make correlation among different aspects of a person's identity more difficult. By removing the tie to a widely used identifier—such as a social security number or driver's license—and enabling the information to be shared granularly but with confirmation that it ties to the individual sharing it, blockchain enables greater privacy by avoiding ties among different pieces of information about oneself that a third party can then aggregate together.

11 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).

V. Privacy Recommendations

With CCPA enacted and CPRA on the horizon, California already has a strong privacy-protecting legal regime. Blockchain is a new technological solution, but it doesn't change the fundamental privacy rights, set forth in the OECD Fair Information Principles, to which individuals are entitled. As noted above, providing those privacy rights isn't incompatible with use of blockchain, whether under CCPA, GDPR, or other similar laws. So at present there is no need to amend or change California privacy law to enable or further promote adoption of blockchain technologies and use cases. That said, it will be important for the legislature to be vigilant in monitoring for potential new issues in blockchain applications related to protecting individuals' privacy that aren't addressed by technical measures or the existing legislative framework.

What is needed, however, is more education about how to use blockchain in a privacy-compliant and enhancing way. The guidance from the European Blockchain Observatory and the CNIL provide a good start, but are obviously tailored to European law. If adopted, CPRA would establish a new California Privacy Protection Agency. If that comes to pass, the California Legislature should task the agency with issuing guidance for both the State and for private entities on how to deploy blockchain in a manner that complies with California privacy laws. In the event that the Agency isn't created, then the Attorney General, as lead enforcer of privacy laws in California, should issue such guidance and be provided the necessary resources to do so.