CARLTON FIELDS

Regulating Privacy on the Blockchain Starts With Understanding the Meaning of "Personal Data"

August 06, 2019

A commonality among recent data privacy regulations (including the EU's GDPR, California's CCPA, and Brazil's LGPD) is that only the storage and transmittal of "personal data" is regulated. These new regulatory frameworks generally define "personal data" (or "personal information") obliquely as elements that relate, by themselves or taken together with other data, to an identified or identifiable individual. As companies across the world explore transitioning data storage onto encrypted, open databases including blockchains or similar technologies, an emerging question has arisen over whether such uses could violate privacy regulations and, counterintuitively, force companies into adopting less secure data storage methods than available through new technologies.

Part of the challenge of applying new technologies to existing regulatory frameworks is definitional. Privacy regulations purposefully employ broad definitions of "personal data" that make it difficult to apply to all types of data. Excluded from most regulations are business-to-business data (B2B), data used solely for household purposes, and "anonymous data," meaning data that has had personal identifiers removed or rendered indecipherable. The exact bounds of these categories remain unclear, and it is not often easy to categorize data as fitting into one category to the exclusion of other, regulated data types.

Privacy regulations are generally technology agnostic and apply to all methods of storage and transmittal, including blockchains. One of the challenges of applying privacy regulations to blockchains is that not all blockchains are equal or employ the same level of security or encryption. Some have open, decentralized, and pseudonymous characteristics, and therefore may or may not be compatible with regulatory frameworks.

Generally, regulators have treated blockchain technologies like cloud computing and view it as just an additional means of collecting and processing data. Accordingly, if data on a particular blockchain cannot be used to identify an individual, then it is generally spared from data privacy regulation altogether. The same is true for data contained on a public, permissioned, or private blockchain.

A good starting point for analyzing the application of any given data privacy regulation to the blockchain (or any new technology) is to ask whether the data can be considered personal data. In some cases, the answer is obvious, like data that identifies the owner of a property. In others, the answer is less clear. One of the most common data elements related to public, proof-of-work blockchains like Bitcoin is the pseudonymous identity of the miners who help to maintain the blockchain. In most cases, this information will consist of alphanumeric characters that are not on their face personally identifiable. This database architecture can be used to maintain a high level of confidentiality; however, if an entity has access to one's private key or can link the information to an individual's identity, then the data may be considered personal data and the entire blockchain may, as impractical and unenforceable as it may be, be subject to regulation.

Such considerations are highly dependent on the architecture and unique characteristics of the blockchain, which is essential to keep in mind when implementing products or services that use distributed and encrypted technologies like blockchains. Indeed, some regulations like the GDPR require entities to build privacy into the design of their products and consider data collection practices and techniques at the outset before venturing into new technologies. Some also require an assessment of the risks associated with the exposure of personal data, which makes sense to do in any event from a business standpoint.

Privacy-by-design principles further dictate that entities employ data minimization techniques to keep as much personal data off the blockchain as possible. This can include the use of commitments, hash keys, ciphertexts, or other sophisticated technologies like zero-knowledge proofs to make the data on the blockchain practically inaccessible. Guidelines from one of Europe's leading data protection authorities in charge of enforcing the GDPR recognize the use of these crypto techniques as the functional equivalent of deleting personal data from the blockchain. As blockchain technology evolves, it is reasonable to assume that data minimization techniques will as well, and additional methods of "deleting" data from the blockchain will surface.

Therefore, to properly assess whether and to what extent data privacy regulation applies to any particular blockchain first requires an answer to this question: Is the data "personal data"? If it can be considered personal data, and this ultimately may vary across regulators and courts, then a given data privacy regulation could apply and all of its requirements should be considered. But if not, then considerable effort could be saved because it is more likely than not that data privacy regulations do not apply to that particular data. Those seeking to implement blockchain technologies in their

business would be wise to keep this in mind when considering whether, and to what extent, to use blockchain technology.

Related Practices

Blockchain and Digital Currency
Cybersecurity and Privacy
International
International Litigation & Arbitration
International: Brazil
International: Cuba
International: Europe
International: Latin America