Navigating Blockchain and Data Privacy

Feb 28, 2020

Categories:

Blockchain and Digital Assets
Blogs

Authors:

Daniel A. Murray
Courtney Rogers Perrin

Blockchains are becoming more prominent in cryptocurrencies like Bitcoin, supply chain applications, and more. Two typical features of blockchains are transparency and immutability. Despite the money flowing into this technology, there are several legal challenges, including the application of data privacy laws. Here are some issues to keep in mind.

Who has jurisdiction?

There are no clear borders when it comes to data privacy or blockchain. Data privacy laws can cover a state (California Consumer Privacy Act) or a group of countries (General Data Protection Regulation "GDPR" in the European Union). And these laws often apply to a subject citizen, regardless of that citizen's physical location. Meanwhile, public (or distributed) blockchains may reside on computers scattered around the world. Private blockchains may reside at a centralized location. But even then, if multiple countries can use that private blockchain, then each country's data privacy laws may apply.

Courts have just begun to address the jurisdictional issues. In the United States, courts are looking at previous case law on websites. Although it's difficult, best practice would be to comply with each local law applicable to your blockchain, including server location, consumer citizenship, and consumer location. To avoid a specific data privacy law, blockchains will likely have to prohibit users and servers from that locale. This could mean blocking all U.S. IP addresses, for example.

Right to "Delete"

Data privacy laws sometimes provide consumers a right to delete data. This poses a challenging feat when the data may reside on millions of computers around the world, the blockchain may have no managing central authority, and it may have been built to be

FBT Gibbons

immutable. Helpfully, pseudonymization of the data can reduce some of the compliance requirements associated with deletion. Under pseudonymization, a piece of data can only identify a consumer when combined with additional data.

Controllers v. Processors

Data privacy laws often distinguish parties that collect and control data from parties that simply hold the data temporarily to complete some analysis. In the land of blockchain, the blockchain itself—particularly if it's a private blockchain—is likely the controller. That raises the compliance requirements.

Right to Transfer

Like the right to delete, a right to transfer implies that consumers can control their data and move it at will. But in blockchain this may not be possible. Again, as with the right to delete, blockchains will want to implement data pseudonymization to avoid the most onerous requirements of data privacy laws.

Chief Compliance Officer – CCO

GDPR requires companies to name a chief compliance officer in some cases. But even if GDPR is not applicable, most companies will need a specialist to monitor its data privacy activities and possible compliance issues. Because data subjects often reside in multiple countries, companies can quickly become subject to multiple data privacy laws. With or without a data protection officer, blockchains should document their efforts to comply with GDPR and other laws.

Learn more about our legal services relative to the FinTech, Blockchain, and Data Privacy ecosystem.

FBT Gibbons