Lex Mundi World Ready

FOLEY HOAG LLP

Lex Mundi Blockchain White Paper Series

Blockchain and Data Privacy

by Christopher Hart, Foley Hoag LLP (Lex Mundi member firm for USA, Massachussetts)

What data privacy concerns should practicioners have relating to blockchain technology? Answering the question involves understanding first the personal information implicated by a specific blockchain application, and then analyzing the relevant legal regimes that govern the personal information.

Personal Information

Data privacy does not implicate all information, but personal identifying information. This means different things in different legal regimes, but it typically does not mean business commercial information, trade secret information, or intellectual property. While these kinds of information are sensitive and can be subject to various regulatory and contractual protections, they are not the kind of information that brings up data privacy concerns.

Rather, information like an individual's name, address, identification number, financial information, health and biometric information, and so on are the kinds of information that implicate data privacy concerns.

Blockchain as used in financial and commercial transactions, or as might be used in robust supply chain technology, might not necessarily implicate data privacy concerns if the information does not contain or cannot otherwise be linked to personal identifying information. In other words, if all a block contains is hashed information about the details of a transaction, but is not otherwise linked to a person, it will not implicate data privacy concerns. But if personal identifying information is provided, or can be linked to an individual, then data privacy concerns will be implicated.

Blockchain Applications

Cryptocurrency and Smart Contracts - Anonymity v. Pseudonimity

Despite its superficial promise of anonymity, as a distributed ledger technology that obfuscates personal and other data but provides information about transactions to every node with access to the ledger, blockchain technology has the potential to create privacy headaches depending on the specific application. Cryptocurrency provides the best (and at this point in time, most relevant) example. The promise of cryptocurrency - and one of its potential dangers - was that it would allow for anonymous transactions. But in reality, blockchain technology in the cryptocurrency space provides pseudonymity. On the one hand, this means that parties can engage in transactions without revealing their actual identities. But if a determined party has access to certain information in the public domain regarding certain transactions, that party might be able to de-anonymize individuals based on the context surrounding those transactions. Pseudonymity, in other words, does not provide a user of blockchain technology with an absolute assurance that her identity will not be discovered.

Smart contracts function much the same way, with the same sort of concerns regarding true anonymity, allowing for transactions to have such information as price and type of good to define the transaction without the need for personal identifying information. But a third party wishing to learn the identity of an individual on either side of a transaction as represented in a smart contract might be able to do so if it is able to locate the appropriate information from the public domain.

Private Blockchain Applications

While the applications we have considered concern public ledgers, where anyone can gain access, private blockchains, which are limited to specific users, dimish some risks but heighten others. Private blockchains diminish the risk that someone on the node can gain access and discover private identifying information using information from the public domain. But private blockchain applications can heighten the risk based on the data obtained. For example, a private blockchain might be used by a health insurance company or health provider to maintain electronic health records (EHRs), which contain personal health information. A private blockchain containing EHR could dramatically increase efficiency by allowing those with access - the insurer and the provider - easy access to the chain of information in a patient's history. But the sensititve of that information would implicate a number of legal regimes and would require robust security to maintain privacy.

Legal Regimes

United States

In the U.S., there is no overarching data privacy protection law at the federal level. Rather, at the federal level, data privacy is regulated by sector specific laws, such as HIPAA for personal health information or the GLBA for banking and financial information. Entities like the Federal Trade Commission have broad law enforcement powers relating to data privacy, but that is based on their protection against unfair and deceptive commercial behavior. In the absence of a federal data privacy law, each state has its own data privacy law, but these tend to focus on data breaches rather than create robust data privacy regimes (California has recently passed a new law that will act as a comprehensive data privacy regime when it goes into effect). To that end, data privacy concerns with blockchain technology in the U.S. concern whether the blockchain is secure (that is, whether it can be or has been subject to a data breach), and whether it contains personal identifying information that is subject to a federal sector-specific law.

European Union

Perhaps the most worrisome aspects of blockchain is the potential application of the General Data Protection Regulation, or GDPR. Under the GDPR, data subjects (that is, any individual in the EU) has a number of data privacy rights, including the right to have personal information corrected or deleted. Additionally, the GDPR creates certain restructions on data transfer across borders - outside of the EU, if a country is deemed not to have adequate data privacy protections, restrictions are placed on transfer to that country.

Blockchain can hardly be thought to be compatible with the GDPR. The nature of the technology simply does not allow for deletion or correction of information. Further, with regard to public blockchains, there is no way to police cross-border transfer of information; information that appears on the blockchain in a new transaction appears on each node wherever that node might be.

In some respects, these concerns are theoretical. To the extent that transactions in a blockchain application do not contain personal information, then GDPR risks are diminished. But a private blockchain will be subject to these restrictions if the ledger is subject to the GDPR and contains private information.

If a company is considering blockchain technology for its data processing and that processing implicates the GDPR, the infancy of both the GDPR and blockchain applications can make it difficult to navigate these difficulties. But EU supervisory authorities (that is, each country's data privacy legal regime) are taking notice. For example, the French data privacy authority recently published guidance on blockchain technology, strongly recommending data minimization (that is, limiting the amount of data that exists in each block). Practitioners should keep abreast of such guidances to best advise their clients.

For more information, contact bd@lexmundi.com.