Blockchain and Privacy: Irreconcilable Differences?

In the race between law and technology, law is the tortoise, technology is the hare. And one of the fastest hares on the tech scene is blockchain.

Blockchain, of course, is the much buzzed about (and little understood) distributed ledger technology underlying Bitcoin and other cryptocurrencies. But its potential reaches far beyond cryptocurrencies into supply chain management, digital rights management, contract execution, prevention of identity theft, maintenance of real estate records, and many other fields where solid proof of transactions is key.

One of the most attractive features of blockchain technology is its immutability, since the "blocks" that make up the blockchain are distributed across a vast number of computers. But that feature can also create headaches for purposes of complying with data protection laws.

Under the EU General Data Protection Regulation (GDPR) that became effective earlier this year, one of the fundamental rights of EU data subjects is the right of erasure (sometimes referred to as the "right to be forgotten"). So how does that right mesh with the immutable nature of blockchain?

At a session of the IAPP's Privacy.Security.Risk conference that I attended in San Diego last month, the outlook for blockchain peacefully co-existing with the GDPR was cloudy. As one speaker noted: "The GDPR assumes you have a central point of control to an individual's personal data, which is the opposite of what a permissionless blockchain does."

The French data protection authority, the CNIL, has just bravely waded into this murky situation with a white paper that is a manifesto of sorts: "Solutions for a Responsible Use of the Blockchain in the Context of Personal Data."

The "concrete solutions" that the CNIL has proposed include the following:

> ● *Determine who is a data controller and who is a data processor.* The distinction between "controller" and "processor" is key under the GDPR. The controller is the party that determines the purposes and the means of the processing; the processor just follows the controller's directions. In the blockchain context, the CNIL has determined that blockchain "participants," who have the right to write on the chain and decide to send data for validation by "miners," can be considered data controllers. Miners, by contrast, are only validating transactions submitted by participants and are not involved in the objects of the blockchain transactions; therefore miners, as well as smart contract developers, may be considered processors.

- ➤ ***Assess whether a blockchain is the right tool for the task.*** Here the CNIL punted, implying that the best "solution" may be no blockchain at all. The GDPR restrictions on cross-border transfers may be especially problematic in the blockchain context, the CNIL suggested. The CNIL did note that a "permissioned" as opposed to public blockchain would help ameliorate the privacy concerns.

- ➤ ***Choose carefully the format under which blockchain data will be registered.*** A couple of GDPR principles are data minimization and data retention period; i.e., only relevant data should be collected, and data should be retained for no longer than necessary. The CNIL acknowledged that these principles run up against one of the primary characteristics of the blockchain, which is that data, once registered on the blockchain, can't be technically altered or deleted. However, the CNIL proposed that various technical solutions be considered, including (i) choosing a blockchain format that minimizes the use of personal data, including using a hash function with a key; and (ii) conducting a data protection impact assessment (DPIA) to help determine whether the residual risks are acceptable from a data protection standpoint.

- ➤ ***Implement technical solutions to the exercise of data subject rights.*** The CNIL readily admits that "it is technically impossible to grant the request for erasure made by a data subject when data is registered on a blockchain." But rather than throw in the towel and conclude that the GDPR right to erasure effectively outlaws use of blockchain, the CNIL suggests that the blockchain data can be made "practically inaccessible" through use of a hash generated by a keyed-hash function or a ciphertext obtained through state-of-the-art algorithms and keys. These technical tools "can make the data practically inaccessible, and therefor move closer to the effects of data erasure."

Perhaps the most important feature of the CNIL paper is that it signals a willingness of this EU data protection supervisory authority to recognize that new technology platforms such as blockchain are inevitable, and therefore data protection laws must be interpreted flexibly to accommodate them. That is a welcome perspective indeed; let's hope the other national supervisory authorities follow suit.