LAW.COM

An ALM Website

July 3, 2018

Blockchain and GDPR — Frenemies?

In a nutshell, GDPR mandates that individuals have access and control over the use and maintenance of their data in certain circumstances, while the foundation of blockchain relies on the immutability of data. On the surface, these concepts seem in direct conflict with each other. This article discusses the points where GDPR and blockchain share common ground, where conflicts may exist and possible approaches for mitigating those conflicts.

By Justin Hectus and Kristy Sambor

Emerging technologies and regulations have the power to create, shape, or kill businesses. The European Union's (EU) General Data Protection Regulation (GDPR) — a privacy regulation with worldwide implications, and blockchain technology — such as Distributed Ledger Technologies (DLT), each embody forces that have the potential for such profound impact. Taken in tandem, the GDPR and blockchain highlight the possibilities and pitfalls of disruption and the importance of cross-organizational collaboration in compliance and innovation initiatives.

In a nutshell, GDPR mandates that individuals have access and control over the use and maintenance of their data in certain circumstances, while the foundation of blockchain relies on the immutability of data. On the surface, these concepts seem in direct conflict with each other. This article discusses the points where GDPR and blockchain share common ground, where conflicts may exist and possible approaches for mitigating those conflicts.

This article appeared in Cybersecurity Law & Strategy, an ALM publication for privacy and security professionals, Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, Corporate Counsel, Internet and Tech Practitioners, In-House Counsel.

Hype Check

With the possible exception of AI-powered robot lawyers, no topics have dominated the legal technology hype cycle more than GDPR and blockchain have in the past few years. This has been for good reason.

The sweeping requirements of GDPR compliance against the backdrop of an increasingly interconnected and online world have forced companies everywhere to focus attention and resources on redefining their information governance and security programs, as well as their relationships with customers and technology providers. Corporations are spending billions of dollars on compliance initiatives and still nearly half of corporations did not expect to be fully compliant with the regulation when it became enforceable on May 25, 2018.

The ripple effects of the regulation have been felt by companies of all sizes and in all geographies. In recent months, a flurry of Data Processing Agreements and Terms of Service updates have been pushed to anyone who touches the data of a company that offers goods or services within the EU or the European Economic Area (EEA) and deals with the personal data of data subjects in the EU.

Blockchain beyond cryptocurrency may still be in the relatively nascent stage, but it has been showcased in real-world use cases including banking, global trade, voting and property records, and has shown promise in the realms of

cybersecurity and healthcare. In fact, in the last year blockchain technology has been deployed to help refugees build digital identities and credit histories to help them obtain employment and rebuild their lives. Every day, companies are finding innovative new ways to utilize the technology.

Of course, with the amount of hype and capital flowing into the space, some companies have focused on capitalizing on this in the short term, such as Long Island Iced Tea which famously warranted to separate these actors from those focused on longer term value creation with blockchain.

On the long-term business potential of blockchain, research and advisory firm Gartner prognosticates that "long term … this technology will lead to a reformation of whole industries." It may be too early to bet the company on blockchain-powered transformation, but expert opinions and investor response both suggest that now is the time to start experimenting with blockchain and DLT.

Common Ground

Blockchain and GDPR have very different origin stories, but they have grown up together and they each reflect the zeitgeist of the last decade in a few key areas:

Consumer Demand for Increased Security

The GDPR may be a privacy regulation, but data protection is a core principle. Controllers, processers and sub-processors are held to high standards with respect to broad cybersecurity concepts and specific breach notification requirements. Blockchain's encryption and decentralized structure makes the network and data highly tamper-resistant and, in theory, less vulnerable to unauthorized modification than a single instance database.

Consumer Demand for Visibility and Control

The GDPR represents a shift to consumer ownership of their own data, requiring companies to provide visibility and control to individuals, on demand. Blockchain is being used as the base technology for dozens of applications focused on consumer control of data from identification to monetization.

Erosion of Consumer Trust In Institutions

The GDPR has made great strides by requiring not only transparency into what companies will do with consumer data, but also mandating clear consent mechanisms to ensure that consumers understand what companies are sharing, with whom, and for what purpose. Blockchain and cryptocurrency came into existence in part because of a loss of trust in financial institutions during the financial crisis. Blockchain continues to be leveraged in ways that bridge the gap in consumer trust in areas as varied as news and insurance.

Conflict

As with most coming of age stories, the tale of these two Generation Z kids is not without conflict. In this case, the GDPR's right to erasure and blockchain's fundamental immutability may be akin to an unstoppable force meeting an immovable object.

Although not absolute, the "right to erasure" is a powerful example of the GDPR placing ownership of data back in the hands of the consumer. This same right presents one of the most significant challenges for companies to operationalize. Legacy systems, backups, and a lack of holistic information governance programs are obstacles to effective search and destroy protocols. Although finding and deleting an individual consumer's data within a single company is possible without fundamentally impacting system functionality, performing that same operation on a blockchain may be impossible.

Blockchain's fundamental tenet is the absolute integrity of the records in the chain, because the block in which each record is stored is inalterable once added to the chain. The same quality that protects blockchain against unauthorized modification prevents erasure of records, even by an authorized and lawful request. This is particularly problematic in public blockchain-based platforms, where any personal information stored on chain is spread network-wide, setting the stage for a profound conflict between this emerging technology and fundamental right to erasure provided by the GDPR. Blockchain solutions that store personal information may be permanently stuck in that state.

Another problem is how the GDPR defines the rights and responsibilities of data controllers, processors, and sub-processors. A controller is anyone who determines the "purposes and means" of the personal of processing data and a processor is anyone who insomuch as touches the data on behalf of a controller. Understandably, these roles often overlap. The distinction between controller and processor can be debated in defined business relationships using mature technologies, but the discussion is likely to get messy in a blockchain solution where every node is arguably a processor or possibly even a controller. All of this has yet to be tested through enforcement action, but fines for noncompliance can be levied against controllers and processors, which could cripple a public blockchain solution that stores even pseudonymized personal data.

The GDPR is forcing conservative companies to rethink their business models and their geographic footprints. Dozens of news organizations, including the *Los Angeles Times and Chicago Tribune* shut down access to their digital content for the EU market as of May 25 and a few ad-tech firms have ceased EU operations to focus on operations in the U.S. and elsewhere. For companies and solutions built on blockchain, the options may be limited. The first such casualty was Parity's ICO Passport Service (PICOPS), which shut down completely on May 24. PICOPS launched just eight months earlier and was a popular service offering a means to validate that the owner of a specific Ethereum wallet had passed a background check. PICOPS specifically cited GDPR as the catalyst for closing shop.

A Path Forward

When considering options for business advantage against the backdrop of competing transformational forces, it is worth remembering that the future is uncertain for all business and experimentation is a valuable exercise. Innovation generally outpaces regulation, but when regulations do catch up, technologies must often pivot to ensure compliance. With this push and pull in mind, companies will be well served to include the concept of "privacy

by design," one of the dictates of the GDPR, in their innovation programs.

Andrew Clearwater, Director of Privacy for the global privacy platform OneTrust, agrees. "When it comes to addressing the risks of new technology, the approach does not need to be new. Our customers often approach these challenges through Data Protection Impact Assessments (DPIAs). Using a DPIA, the nature, scope, context and purposes of the processing is revealed, and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data can be evaluated."

Whether the focus is blockchain or other new technologies like workflow automation, voice assistants, smart bots, AI or even something as seemingly straightforward as cloud storage, DPIAs and Privacy Impact Assessments (PIAs) should be integrated with existing processes. If corporate innovation initiatives start and live in Jira, for example, DPIAs and PIAs can be triggered and linked early in the development project in Jira and linked to templates in OneTrust. Clearwater advises that OneTrust has seen "the development of triggers within their tool for project management that allows for streamlined workflows that won't detract from existing work" which helps with company-wide adoption of the practice.

With all of the deserved hype surrounding blockchain and deserved compliance focus surrounding GDPR, conflicts can result in a potentially messy cleanup if not addressed early in the development process. Potential options for utilizing DLT and blockchain solutions and navigating GDPR challenges include:

- Increased use of private or enterprise blockchains, which are blockchain systems used by one company or amongst companies in a particular industry. Unlike public blockchains, which provide decentralized utility and access to as many users as possible, private and enterprise blockchains limit the dissemination of personal information to just one company or a limited number of companies. In reducing the scale of the chain, fewer individuals have access to sensitive information and the possibility of data breaches significantly diminish.
- Use of pseudonymization techniques in combination with data stored off-chain. In order for data to be considered pseudonymous under GDPR, the data must "no longer be attributed to a specific data subject without the use of additional information" (GDPR Art. 4(5)). Pseudonymous data, unlike anonymous data, therefore still allows for re-identification. While pseudonymization techniques make it more challenging for users to identify data subjects, it does not scrub all identifying personal information. Pseudonymization with pointers to personal data stored off-chain in a manner which allows the personal data to be destroyed and thus removes the link to the data on the chain and renders it anonymized may allow a user to remove all of their personal information from the chain, as required by the GDPR's right to erasure.
- Development of mutable blockchains. For example, the R3 Corda team is currently exploring "sophisticated anonymization techniques" that would allow users to edit and/or delete their personal information shared on a private blockchain, giving them 100% control over their own data. This "self-sovereign solution" would "ensure provisions in GDPR that allow individuals to access and correct their personal data would be fulfilled and provides a compliant solution to restrict data processing."
- Reliance on exceptions to the right to erasure. The right to erasure is not absolute in all circumstances. For instance, the right to erasure does not apply to the extent that processing is necessary for compliance with a legal obligation that requires processing by Union or Member State law, and it does not apply to the extent that processing is necessary to establish, exercise or defend legal claims. (GDPR Art. 17(3) (b) and (e).) Other exceptions may also apply. Businesses might reject a request for erasure of personal data based on recognized exceptions in the GDPR, but there is little guidance in this area and whether these exceptions will successfully apply to blockchain solutions has yet to be tested.

Conclusion

Ultimately, lawmakers and technology pioneers may meet in the middle with blockchain solutions that store as much personal data off chain as possible and privacy regulations that allow for a variation on the right to be forgotten that can accommodate this new, potentially transformational technology. In the meantime, businesses would be advised to incorporate a focus on security and privacy in their innovation initiatives. As suggested by OneTrust's Clearwater: "Privacy cannot be ensured through regulatory compliance since the law always lags advancements in technology. Instead, it makes sense to apply specific tools like automation of DPIAs in combination with a flexible framework like Privacy by Design to ensure that there is an operational approach to privacy embedded within the business."

Justin Hectus is the CIO and CISO of Keesal, Young & Logan where he oversees a variety of operational functions including the direction of the firm's IT vision, strategy and execution. A member of this publication's Board of Editors of *Cybersecurity Law & Strategy* and a two-time ILTA Distinguished peer award winner, Justin regularly advises KYL's clients and attorneys on the opportunities and challenges associated with a rapidly changing technology ecosystem. ***Kristy Sambor*** is an associate with Keesal, Young & Logan and a member of KYL's Cybersecurity and Privacy law practice. Her work involves advising businesses of all sizes on data privacy compliance, cybersecurity, and data breach response. *This information has been prepared for informational purposes only and is not intended to be legal advice. Individuals and/or companies should not act upon this information without seeking professional counsel from an attorney.*