



Mar 18, 2021

Categories:

[Blockchain and Digital](#)

[Assets](#)

[Blogs](#)

[Technology Blog](#)

Authors:

[Daniel A. Murray](#)

[Courtney Rogers Perrin](#)

Blockchain and Art Provenance: Five Data Privacy Challenges

Distributed ledger technologies (DLTs) are becoming more prominent with applications across supply chains, including art provenance. Several entrepreneurs have stepped into the space, developing ways to associate a blockchain to a physical item.

One system, Verisart, allows artists to create a certificate of authenticity for an artwork, including a link to the owner's blockchain address. Another, Blockchain Art Collective, uses an NFC-enabled certificate of authenticity that writes data about a piece to a blockchain database. The certificate is tamper-resistant and attached to the artwork; any evidence of tampering would alert a purchaser to provenance problems.

A third system, Codex, works with art purchasers to create a rigorous provenance record and receive a tamper-resistant sticker linked to their blockchain. When the item is subsequently sold, the record can be transferred to the new owner. And a fourth, Artory, uses experts who, upon validating a piece of art, issue a registration certificate on the Ethereum blockchain. The art owners are kept anonymous, though the registry is publicly available.

Despite the real money flowing into these art provenance/blockchain solutions, there are several challenges, including the application of data privacy laws across multiple jurisdictions. Here are some issues to keep in mind.

Who Has Jurisdiction?

There are no clear borders when it comes to data privacy or blockchain. While DLT and art sales are global, data privacy laws can cover a state (California Consumer Privacy Act) or a group of countries (General Data Protection Regulation in the European Union). These laws can even apply to a citizen regardless of that citizen's residence. Public (or distributed) blockchains may reside on computers scattered around the world, while private or centralized blockchains may be domiciled in one location. But even

then, if citizens of multiple countries can use that private blockchain, then the data privacy laws of each citizen's home country may apply.

Courts have just begun to address the jurisdictional issues. In the United States, courts are looking at previous case law on the domicile of websites as precedential. Although 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, art provenance blockchains will likely have to use geofencing to prohibit users and servers from that locale. This could mean blocking all U.S. IP addresses, for example.

Right to "Delete"

Many data privacy laws protect consumers and provide a right to delete data, a challenging feat in blockchains where the data may reside on millions of computers around the world, may have no managing central authority, and may have been built to be 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, but whether the blockchain art provenance solutions can meet the pseudonymization requirements is to be determined.

Controllers v. Processors

Data privacy laws tend to distinguish parties that collect and control data from parties that simply complete an analysis of the data on behalf of someone else. In the land of art provenance, the blockchain itself – particularly if it's a private blockchain – is likely the controller. That raises compliance requirements even if the blockchain provider might want to call itself a service provider or processor.

Right to Transfer Data

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

Chief Compliance Officer

Most companies will need a specialist of some kind to monitor their data privacy activities and possible compliance issues. And 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, art provenance blockchains should document their efforts to comply with GDPR and other laws.

It's an exciting space, and our Frost Brown Todd team will continue to provide updates regarding the interplay of [blockchain technology](#), art provenance, and [data privacy](#). Please contact [Daniel Murray](#) or [Courtney Rogers Perrin](#) if you have any questions or comments.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.