

Overheard at the Disruptive Technologies Legal Summit 2021

OCTOBER 8, 2021

Winston & Strawn and the Berkeley Center for Law and Technology held the fourth annual [Disruptive Technologies Legal Summit](#) virtually on September 14. In case you missed it, below are our favorite key takeaways from the Summit. Select recordings and supporting materials can be found [here](#).

CRYPTO HAS ESTABLISHED ITSELF AS A VIABLE ALTERNATIVE TO CURRENCY.

1

THE UNITED STATES' REGULATION BY LITIGATION AND THE ABSENCE OF TRANSPARENCY HAVE PUT THE COUNTRY'S ECONOMIC POWER AT RISK, CONSIDERING THE ADVANCES OTHER NATIONS ARE MAKING IN CRYPTO. THESE CURRENCIES CAN POTENTIALLY DISRUPT THE GLOBAL BANKING AND FINANCIAL ECOSYSTEMS AND RAISE CRITICAL ISSUES SURROUNDING FINANCIAL STABILITY AND PRIVACY.

2

Regulators have taken notice of the transformative disruptive impact decentralized finance (DEFI) has had on the world, including in the lending arena, and are looking to rein in what they perceive to be a "Wild West" frontier.

Providers of financial products and services as well as individual investors and traders in this space should be prepared to traverse a new regulatory regime which may, at least as an

initial matter, include ill-fitting protocols and notions imported from centralized governance models.

3

Banks may soon have a newfound incentive to build technology pipelines to custody cryptocurrency and to provide customers more expedient access to their crypto assets.

This is assuming the new head of the Office of the Comptroller of the Currency implements the interpretive letters currently “under review” that conditionally authorize digital asset trust companies.

4

Blockchain technology and smart (or automated) contracts present a dizzying array of use cases in fields as varied as cybersecurity, voting, title insurance, supply-chain management, and commercial banking.

Of late, major financial institutions and clearinghouses have devoted significant resources to exploring this technology to facilitate the speed, efficiency, and reliability of trading more conventional financial instruments such as equities and derivatives. However, widespread trading on a public blockchain or through smart contracts poses its own set of risks that could—in the absence of thoughtful design, meaningful control, and reliable, trustworthy non-parties—introduce significant instability into financial markets.

5

The increase in trading varying digital assets has been accompanied by significant challenges for economists, policymakers, and especially regulators, charged with applying dated legal paradigms to these new financial products.

Although often described as a balance between “innovation” and “investor protection,” the real story is more complicated and involves considerations of equity, financial stability, and even national security.

6

Identifying who owns “the data” from a legal and regulatory standpoint is key to unlocking and

realizing value from investment in digital technology innovations.

Regulators are not necessarily looking to jump straight to a fine every time a company finds itself in conflict with the law, but a focus on prevention and prompt remediation is critical.

7

Companies should incorporate a data privacy assessment and risk analysis at the beginning of any serious discussion about an investment in data involving patients—even if the data appears to be aggregated and de-identified.

Understanding where you started is crucial to assessing the potential effects as the commercial project grows and evolves.

8

It is critical to implement and operationalize data security by design into the development of new technologies.

Embedding data privacy expertise early in the design process and across functional teams can help future-proof technology.

9

Leading companies are employing ethical frameworks where there is a gap between technology and legal requirements to meet consumer expectations and avoid privacy pitfalls.

10

Companies building AI models should monitor and make sure their voices are heard in connection with the regulatory changes and AI legislation on the horizon around the world...

...some of which is proposing to gain access to source code and make onsite inspections of U.S. companies when there is an AI bias incident.

11

Legal counsel, data scientists, and company leaders must work across business units to ensure that policies and procedures are in place early to detect and mitigate AI bias before products reach consumers.

Every AI system is going to reflect patterns in the data it is trained on, but patterns of bias such as under-representation, measurement errors, or undesirable correlations can be spotted in the data before a model is even trained.

12

China appears to be in the lead of the modern-day “space race” for quantum technology.

The United States has an opportunity to secure its place in this technology through early investment in this technology to secure its place in this technology. Eventually, quantum information science will be commercially available.

13

As the United States continues to develop its broadband technology, it needs to ensure access to all citizens.

Broadband is not available to all people in the United States—universities in rural areas, like many historically Black colleges and universities, are among those with limited access.

3 Min Read

Related Topics

[Disruptive Technology](#)[Technology](#)[Health Care](#)[Data Privacy](#)[FinTech](#)[Artificial Intelligence \(AI\)](#)[Emerging Technology](#)

Related Capabilities

[Litigation/Trials](#)[Transactions](#)[Patent Litigation](#)[Privacy & Data Security](#)[Technology, Media & Telecommunications](#)[Cryptocurrencies, Digital Assets & Blockchain Technology](#)[FinTech, Banking & Payments](#)[Financial Services](#)[Artificial Intelligence \(AI\)](#)

Related Regions

Related Professionals



George Mastoris



Krishnan Padmanabhan



Saranya Raghavan



T. Reed Stephens



Susannah Torpey



Danielle Williams