OPPORTUNITY #41

What if digital realities rewrote liability laws in the real world?

LAW AND ORDER FOR WEB 3.0

New models of liability emerge from our online lives and reshape liability laws and regulations in the real world.

MEGATREND
Digital Realities

TRENDS
Cybersecurity
Legal Transformation
Metaverse

SECTORS AFFECTED
Cyber & Information Security
Data Science, AI & Machine Learning
Financial Services & Investment
Immersive Technologies
Insurance & Reinsurance

WHY IT MATTERS TODAY

A legal liability arises when a party has certain responsibilities towards another party in a given area and this should be no different for digital realities, avatars, all parties involved in the associated online flows of goods and services and the value they generate. Cybercriminals seek to exploit human or security vulnerabilities to steal data, passwords and, more directly, money. From hacking and phishing to ransomware and Denial of Service (DoS),[686] cyberattacks can be emotionally and financially devastating with victims displaying mental health symptoms of anxiety, depression and paranoia.[687]

Just over $3.2 billion of cryptocurrency was stolen from various exchanges, platforms and private entities.[688] As FTX – one of the world's largest cryptocurrency exchanges – filed for bankruptcy on 11 November 2022, transfers and deposits were being made into what was perceived as anonymous decentralised finance (DeFi) wallets.[689]

Like non-fungible tokens (NFTs), decentralised finance (DeFi) wallets and platforms — part of digital realities — also face attacks that arise from vulnerabilities in underlying protocols or smart contracts. An analysis found that over half of the value stolen from DeFi protocols happened by exploiting vulnerabilities in code in 2021.[690] Besides security breaches, other reasons for theft include flash loan attacks.[691] This type of attack occurs through the use of funds obtained through a flash loan – a service provided by many DeFi platform exchanges – to manipulate the price of cryptocurrency tokens across platforms. The attacker then sells all their tokens at once at a profit.[692]

On average globally, the cost of a data breach was $4.35 million in 2022, although in the United States the figure was $9.4 million.[693] The share of breaches caused by ransomware grew by 41% in 2021, and this type of breach took 49 days longer than average — 277 days in 2022 — to identify and contain.[694]

Microsoft processes 24 trillion signals every 24 hours and its security solutions (e.g. those built into Windows) blocked billions of attacks on its customers in 2021.[695] Tracking more than 35 unique ransomware families and 250 unique threat actors across the globe plus those who participate in the rising ransomware-as-a-service (RaaS) gig economy,[696] more companies are taking a zero trust approach to security to reduce both the number and scale of cyberattacks.[697]

THE OPPORTUNITY

Avatars bartering or exchanging virtual goods and services in fully digital worlds are a long way from what most legal and judicial systems are designed to manage.[698] As more users and businesses move to or start up in digital realities, there will inevitably be a need for systems to define and protect rights and clearly outline liabilities.

Existing laws and regulations could be reviewed and a new global framework for legal liability could be defined and built into future legislation. Crossing multiple jurisdictions and liabilities, this effort could bring together a partnership of governments, legal researchers and practitioners, software programmers, investors and regulatory bodies, paving a new way of thinking about and transacting in digital realities.

Real-world legal systems may not be easily transferable to digital realities. Moreover, given the transnational nature of digital realities and the novel forms of services, goods, currencies and entities found within them, the challenge – as acknowledged in Europe[699] – is non-trivial. When it comes to fraud, identity theft, defamation and crime,[700] it is currently unclear how legal liability would apply, who it would apply to, what laws and regulations would be applicable, and which court(s) of law would be used to enforce actions and penalties.

BENEFITS

Liability protection and enforcement in digital realities. Gains in efficiency, time and cost-savings by reducing the need for specialised legal research and case development.

RISKS

Tensions between nation-states' legacy systems (designed for physical entities) and emerging digital realities, causing gaps and conflicting approaches that leave many in legal limbo with contradictory outcomes.

Over

$3.2 BILLION

of cryptocurrency was stolen from various exchanges, platforms and private entities