Credit: 1STunningART/Adobe Stock

ANALYSIS

'Akin to the Wild West': Attorneys Warn of Cybersecurity Concerns for Firms in the Metaverse

Cybersecurity and privacy attorneys urge law firms and individuals to 'do their homework' before entering the metaverse, warning them of a lack of uniformity and few means of redressal.

February 24, 2022 at 10:30 AM

5 minute read

Cybersecurity

Isha Marathe
Legal Tech Reporter

For a market projected to outstretch to nearly $800 billion within the next two years, it is certainly no surprise that everyone from McDonald's to Nike to ambitious law firms are setting up shop in the "metaverse."

Of course, like with the World-Wide Web in the 1990s—which today's metaverse is often compared to due to the internet's initial ethos of "no monolithic leader"—the "bad guys" in a new world are seldom far behind the early boom of progress. Indeed, the same qualities that make trademarks and properties in the metaverse so appealing to businesses and individuals—decentralization, digital ownership and embarking into the "next frontier"—might be the ones that make them susceptible to looming privacy threats.

For law firms venturing into the metaverse, their repository of clients' sensitive information might make the stakes even higher.

Data privacy and cybersecurity attorneys say there are steps entities can take to protect themselves as they plunge into the hype of the metaverse, being mindful that in its current state, the space is unregulated and brimming with data and cryptocurrency ripe for the taking.

Founding member of the first personal injury firm in Decentraland, New Jersey-based Grungo Colarulo, attorney Richard Grungo said the big concerns in the space are of gauging the security of digital wallets, understanding the evolving terminology, and scrutinizing the "grey areas" between different "worlds."

"There is so much change going on in this world so quickly it's akin to the Wild West," Grungo said. "In any emerging technology, there is going to be a need for identification of risks, identification of your risk profile and then what you can do to minimize it."

One of the areas Grungo and his firm especially are watching is virtual wallets. In order to purchase currency, one needs a digital wallet to then go about storing their NFTs and cryptocurrency.

“When we purchased our first piece of property in Decentraland, it was a cumbersome process,” he said. “Each world has its own currency and that brings conversion rates into play. It’s a lot to learn. When you buy property and hit send on your digital wallet, you hold your breath, keep your fingers crossed, and wait for the confirmation that the payment went through.”

Theoretically, Grungo anticipates a scenario where an uninformed person might purchase and store their currency in a wallet that may actually be a scam, standing to lose significant sums in the process in what he calls a “crypto robbery.”

Perhaps the more formidable reality is that in a situation such as Grungo’s hypothetical, which has certainly happened before, a decentralized platform means there isn’t much in the way of redressal. There are no “police” or “authorities.”

Grungo said his advice to firms looking to open offices in the metaverse would be to be vigilant in their research, highlighting that the space as it is today is largely lacking in uniformity.

“Knowing the terminology and doing your homework into what world is right for you is going to be the best means for protection,” he added. “Because new software, new apps, new products, and words coming out each day—the gaps in between them, that’s where the holes will be that guys will capitalize on.”

When a technological space is so fast advancing, attorneys encourage firms looking to make the entry to keep an eye on what’s coming, because the future metaverse and its cybersecurity risks will likely look different from today.

Perkins Coie privacy and technology partner Charlyn Ho encourages a step back to reassess what those interested would consider the “metaverse” to be. She refers to today’s version as the “traditional metaverse,” and she envisions a more full-body immersive experience in the coming years as the term comes into fruition, opening doors for immense private data logged into virtual reality.

“Even with the more traditional immersive technology that exists today, it involves a lot more sensitive data about peoples’ homes and their biometrics,” Ho said. “Any type of commercial technology collects way more data than an Xbox or PlayStation controller would.”

Ho said she does not think many users entering the space fully grasp the risks associated with the metaverse and its future, risks that might apply to clients and lawyers alike.

“We have privacy lawyers continuously struggling with how to provide more information to the consumer so they can make their own decisions about their own data or their children’s data,” she added. “Average consumers aren’t able to parse 100 different 5G notices as they pass from one [metaverse] store to another, just as you would in a real mall.”

While Ho anticipates this will take some time, she and Grungo agree that the future of cybersecurity in the metaverse will rely on interoperability between different “worlds.” Until there is a set of privacy regulations or increased uniformity between the digital platforms, users are going to have to be independently careful.

Attorney Evan Schein of Berkman, Bottger, Newman & Schein also encourages any law firm seeking to open an office in the metaverse to first hire a cybersecurity firm to advise them.

“In order for [the metaverse] to be a place where potential is fully realized, it is going to have to provide protection,” Schein said. “Educating yourself about the risks is the only way to protect yourself as of right now.”