HUNTON ANDREWS KURTH

Lawyer Insights

Privacy and Cybersecurity Risks in the Metaverse: 5 Steps to Protect Your Data

To succeed in the metaverse, businesses must consider how they will collect, use and manage data as they enter this uncharted virtual territory.

By Lisa Sotto and Samuel Grogan
Published in Legaltech News | April 26, 2023


As the metaverse soars in popularity, researchers estimate that this new virtual environment could generate global revenues of $13 trillion by 2030. The metaverse promises to augment and digitally disrupt a broad range of sectors, including retail, gaming, media and entertainment, banking and financial services, real estate, and insurance.

Companies are taking note of the massive potential of the metaverse and, according to one study, investment in the metaverse surpassed $120 billion in the first half of 2022 alone. It is clear that the metaverse will offer a plethora of opportunities for new business models, products and services. It is also clear that data is the fuel that will power these new opportunities. To succeed in the metaverse, businesses must consider how they will collect, use and manage data as they enter this uncharted virtual territory.

With the data-driven opportunities of the metaverse come a host of novel privacy and data security risks and legal compliance challenges. Laws and regulations designed to address issues raised by new technologies often lag behind their rapid development, and the metaverse is no exception. For instance, many countries are currently drafting laws to govern the development and deployment of AI, and proposals to regulate the collection and use of biometric data continue to proliferate across the globe. In addition, a wave of new comprehensive privacy laws continues to take the data world by storm.

In the metaverse, many of these laws are potentially relevant. Moreover, policy experts continue to debate the need for metaverse-specific data laws. Despite the current dearth of specific legal guidance, as more businesses plunge into the metaverse and virtual life becomes mainstream, companies will need to move forward to address metaverse-related privacy and cybersecurity risks.

Here are five steps companies can take now to proactively protect data in the metaverse:

1. Adopt protections before entering the metaverse. Before setting up shop in the metaverse, businesses should seek to understand what data they plan to collect, use and share in the metaverse and for what purposes. Creating an inventory of information assets and preparing data flow maps to understand the lifecycle of data generated in the metaverse is a critical first step. Having this knowledge will enable a business to make strategic decisions regarding what information needs to be safeguarded from both a consumer protection and business perspective.

Privacy and Cybersecurity Risks in the Metaverse: 5 Steps to Protect Your Data
By Lisa Sotto and Samuel Grogan
Published in Legaltech News | April 26, 2023

Moreover, Privacy by Design (i.e., considering data privacy at the design stage and through the development of product and service offerings) becomes more important than ever in the metaverse. Companies that treat the metaverse as a digital playground or innovative testing lab without due regard for information protection will likely have a short-lived experience in the metaverse—particularly given the importance of user trust in a world where information collection is ubiquitous.

2. Assess risks associated with new metaverse offerings and implement appropriate mitigation measures. Product and service offerings in the metaverse undoubtedly will create novel risks for companies that play in the space. For example, companies will need to balance requirements related to the processing of sensitive personal information, including biometric data, in an environment that is predicated on the collection and use of physiological data. Conducting Privacy Impact Assessments can serve as a useful tool to identify relevant risks and corresponding mitigation measures.

Businesses should consider issues such as the volume of data they will collect in the metaverse and the purpose of the data collection (for example, is the data necessary to provide the relevant services?); from whom the data will be collected and with whom it will be shared; information that may be inferred from the data collected and how the inferred data may be used; whether appropriate notice has been provided to individuals about the business's data practices in the metaverse and the method of delivering this notice; and additional security measures that may be needed beyond existing controls to protect data in the metaverse.

3. Build a privacy program that adheres to common global principles. It is not clear how—or which—existing privacy laws will apply in a borderless virtual world. For example, if a California resident meets with an EU resident in a meeting space in the metaverse that is managed by a multinational company that conducts business in California and the EU, does the CCPA apply to the data associated with this interaction? Or the GDPR? Or will the metaverse be viewed by lawmakers as its own jurisdiction governed by future metaverse-specific laws?

Given the uncertainty as to which privacy laws will apply in the metaverse, companies entering the metaverse should build an accountable privacy framework that adheres to common global principles. Such a framework should enable appropriate transparency (i,e., notice and choice), facilitate the exercise of individual data protection rights, integrate appropriate security safeguards and incident response measures, adopt a risk-based approach to privacy protection and responsible innovation, and ensure accountability for data processing in the metaverse.

4. Implement appropriate data security protections in the metaverse. Data security is critically important to success in the metaverse, particularly given the high potential for cyberattacks of every kind (such as social engineering, data breaches, virtual identity and digital property theft, account takeovers, hacking of VR and AR devices, and data integrity risks). As the metaverse evolves, new threats inevitably will emerge. The CIS Critical Security Controls provide a useful set of recommended actions to consider as part of a robust metaverse cyber defense strategy.

As a starting point, companies should focus on secure software development. Secure coding, rigorous software testing and appropriate account security features should be top of mind for all metaverse businesses. In addition, certain technologies can help mitigate anticipated security risks in the metaverse. Use of the blockchain, for example, can aid in preventing the theft of digital property such as NFTs, and AI technology can assist in fraud detection and prevention. As the metaverse takes shape and new

security threats are identified, companies should work together to develop a set of metaverse-specific protocols to guide best practices for data security in the metaverse.

5. Respond when things go wrong in the metaverse. Security incidents are inevitable in the metaverse, in large part due to the novel opportunities this virtual environment presents to threat actors. Companies that operate in the metaverse should adapt their incident response plans to anticipate new challenges and threats they are likely to encounter in the metaverse. Businesses also should consider conducting tabletop exercises in the metaverse to prepare for cybersecurity incidents in this novel environment.

One example of an area that can be explored through a metaverse tabletop, for example, is which data breach notification laws will apply in the event of a compromise of personal data. And how will notice be provided to affected users? Which regulators will be notified? These questions and others should be considered in advance of an actual cybersecurity incident in the metaverse. On the data privacy front, there should be recourse for users who are the subject of metaverse-related privacy infringements and data misuse. Businesses operating in the metaverse should consider in advance how they will address these sorts of violations.

The metaverse is an evolving concept. Companies diving into this new environment will need to be flexible and agile—they will need to adapt their privacy and cybersecurity programs over time to stay in step with relevant technological and legal changes. While the regulatory landscape concerning the metaverse undoubtedly will develop over time and businesses will need to keep current on legal developments, those that take a proactive approach to addressing privacy and cybersecurity risks in the metaverse are likely to enjoy long-term success in this new virtual land of opportunity.

Lisa Sotto *is chair of the firm's global privacy and cybersecurity practice group and managing partner of the firm's New York office. In her practice, she assists clients in identifying, evaluating and managing risks associated with privacy and data security practices, counseling them on a wide range of issues from U.S. state and federal privacy and data security requirements to security breach notification laws and global data protection laws (including those in the EU, Asia and Latin America). She can be reached at 212-309-1223 or LSotto@HuntonAK.com..*

Samuel Grogan *is an associate in the firm's global privacy and cybersecurity practice group in the firm's New York office. He can be reached at +1 (212) 309-1385 or SGrogan@HuntonAK.com.*