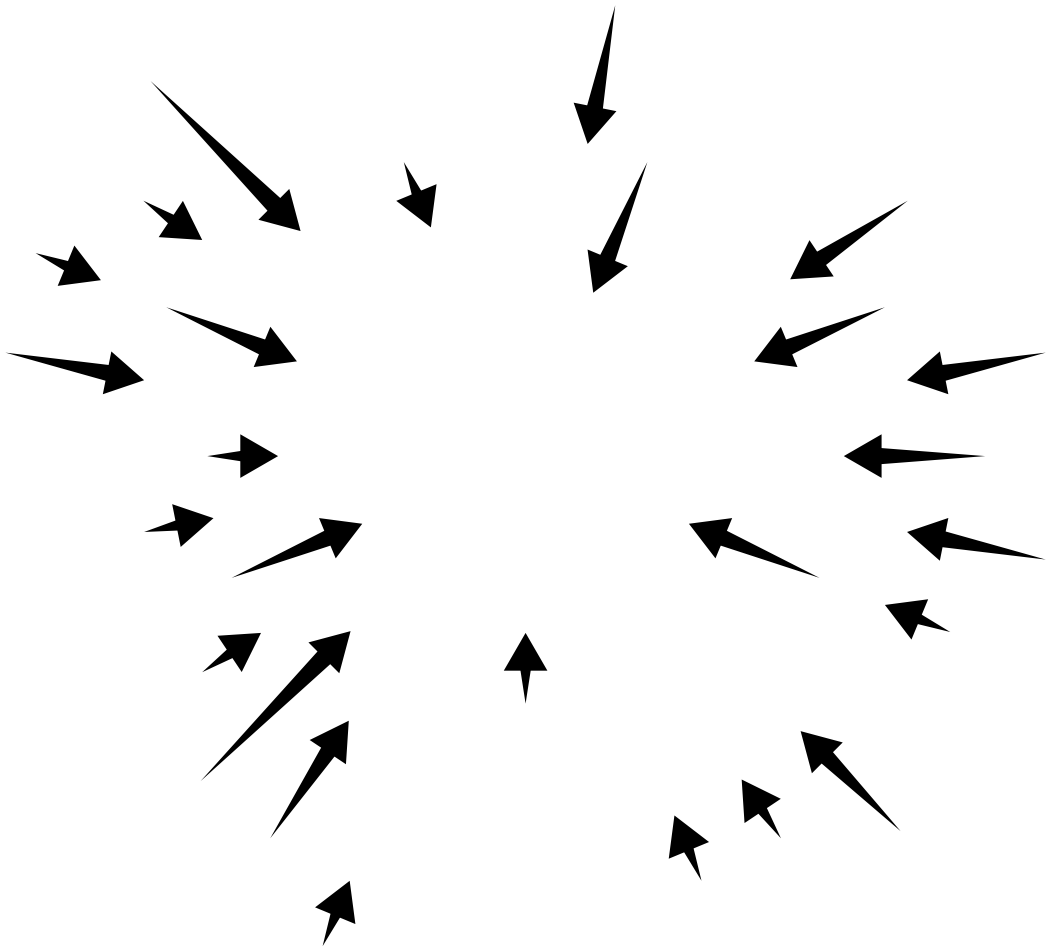

COMPLEX TECHNOLOGIES CONVERGE: PRIVACY AND CYBERSECURITY CONSIDERATIONS FOR ARTIFICIAL INTELLIGENCE IN THE METAVERSE

BY GARYLENE JAVIER

& CHRISTIANA STATE

Garylene "Gage" Javier (CIPP/US) is a Privacy & Cybersecurity associate with Crowell & Moring and based in Washington, D.C. Leveraging her scientific and business background, Gage counsels her clients in understanding, navigating, and responding to complex privacy and cybersecurity issues affecting multinational organizations, including the full lifecycle of privacy program development, privacy and cybersecurity regulatory compliance, and incident response. In addition to her compliance counseling practice, Gage represents clients in technology-related litigation. She writes and speaks on a variety of today's emerging technologies including biometrics, artificial intelligence, the metaverse, and Web3. Gage is a mayoral appointee to the District of Columbia Innovation and Technology Inclusion Council and Vice Chair of the American Bar Association's TIPS Cybersecurity and Data Privacy Subcommittee.

Christiana State (CIPP/US/E) is a senior counsel in Crowell & Moring's San Francisco office and a member of the firm's Corporate and Privacy & Cybersecurity groups. Christiana focuses her practice on counseling clients on technology and privacy matters. Christiana leverages a combination of in-house counsel experience and electrical engineering training to guide emerging technology companies through transformational growth stages. Christiana represents technology companies, from start-ups to multinational corporations, in various industry segments, such as: AI/ML, cloud services, biometrics, semiconductors and computing architectures, gaming, AR/VR, drones, and EV charging. She also advises AI researchers on world-wide data collections and processing for training/validating machine learning models and user studies. Christiana is an adjunct professor at the University of San Francisco School of Law, where she teaches a Privacy and Technology course.

Visit www.competitionpolicyinternational.com for access to these articles and more!

COMPLEX TECHNOLOGIES CONVERGE: PRIVACY AND CYBERSECURITY CONSIDERATIONS FOR ARTIFICIAL INTELLIGENCE IN THE METAVERSE

By Garylene Javier & Christiana State

Technology is advancing at a rapid pace and at the forefront of this evolution is artificial intelligence ("AI") and the metaverse. AI systems have access to vast amounts of personal data and the metaverse offers a new platform for social interaction and commerce. As the use of AI becomes increasingly ubiquitous and the metaverse continues to evolve, organizations should contemplate the implications posed by the use of AI in the metaverse, including: 1) data privacy concerns, 2) algorithmic and automated decision-making bias, 3) cybersecurity threats, and 4) regulation.

01
OVERVIEW

Technology is advancing at a rapid pace and at the forefront of this evolution is artificial intelligence ("AI") and the metaverse. AI systems have access to vast amounts of personal data and the metaverse offers a new platform for social interaction and commerce. As the use of AI becomes increasingly ubiquitous and the metaverse continues to evolve, organizations should contemplate the implications posed by the use of AI in the metaverse, including: 1) data privacy concerns, 2) algorithmic and automated decision-making bias, 3) cybersecurity threats, and 4) regulation.

02
WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence ("AI"), broadly, is the simulation of human intelligence processes by machines, especially computer systems.[2] AI developers use algorithms and statistical models to "train" the AI system to generate conclusions. This requires the ingestion of significant volumes of data collected from various sources and incorporated into the instruction of the AI system. The "training" results in the ability for AI to execute tasks such as recognizing images, understanding natural language, making decisions, and playing games.

There are different types of AI,[3] including:

· Reactive AI (reacts to the environment, but has no memory and is not self-aware);
· Limited memory AI (ability to absorb learning data and improve over time);
· Theory of mind AI (machines would have the capability to understand and remember emotions and adjust behavior based on those emotions); and
· Self-aware AI (aware of emotions and mental states of others, but also their own).

As of today, the most used and developed AI are reactive and limited memory AI, while others have not yet been effectively developed.

03
WHAT IS THE METAVERSE?

The "metaverse" is not one place. Rather, the term refers to a virtual world or a shared virtual space where physical and virtual reality converge and allow users to, among other things, socialize, experience new forms of entertainment, and engage in commerce. Developers can create their own versions of this interactive and immersive technology environment in which user can engage virtually using devices such as virtual reality headsets ("VR headsets").

04
DATA PRIVACY

Privacy issues should be contemplated throughout each phase of the use of artificial intelligence in the metaverse. This includes the AI training phase, use within the metaverse, and ongoing updates to the AI system.

A. AI Training Phase

When developers initially train the AI system, they rely on large data sets to perform specific tasks or make decisions based on data inputs. These data sets generally represent the issue the AI system is meant to solve and as the system goes through the iterative process of testing the output for accuracy, developers adjust the algorithms (weights) to more precisely analyze the data set to subsequently produce the desired outcome. The use of large data sets raises issues of data ownership, appropriate disclosures, and protection of personally identifiable information ("PII").

Data can be sourced from world-wide data collections and processed for training and validating machine learning models and user studies. Such collections of information may be gathered from third-party data brokers or the data owners themselves. Organizations using these data sets inherently must rely on the representation that their data sources acquired the appropriate permissions from data owners for data use, sale, or sharing.

These data sets may include personally identifiable information. However, several state privacy laws require that no-

2 https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

3 https://builtin.com/artificial-intelligence/types-of-artificial-intelligence.

tices be provided at collection, giving individuals the ability to understand, for instance, why their information is being collected, how it is used, and whether it is shared with other entities. For example, the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act of 2020 ("CPRA"), which was the first comprehensive U.S. privacy legislation, provides: "A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of . . . [t]he categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared."[4] Unless the organization developing AI acquires data directly from known data owners, it is challenging to ensure that proper privacy disclosures were issued at the time data was collected.

Accordingly, AI developers should consider the origin of its data sets and assess whether they are reasonably confident that the appropriate disclosures were provided at the onset of collection, and subsequently, whether incorporation of the data into the training and machine learning process is appropriate. In addition, depending on the nature of the data and the uses for such data, it if sometimes necessary to actually obtain consent from the individuals before using such data for machine learning model training.

B. Data Use in the Metaverse

The metaverse provides individuals a platform to engage in commerce and immersive experiences such as gaming within the virtual space. As world building often uses artificial intelligence and user avatars, artificial intelligence may be used to interpret an avatar's or user's actions in order to progress throughout the environment. Such behaviors are often captured by hardware such as VR headsets and handheld gaming devices. Information from these devices can include, among other things, device ID numbers, geolocation, biometric data, environmental data, and behavioral data. In instances where organizations develop a virtual presence, such as a retail store within a metaverse platform, the in-person shopping experience is replicated in the virtual space. Here, natural language recognition AI could be leveraged, and text or voice data is ingested to train the AI system to develop more realistic customer interactions.

"The metaverse provides individuals a platform to engage in commerce and immersive experiences such as gaming within the virtual space

In both examples, data may be transferred from the user hardware to the retailer or game developer as well as the organization whose metaverse platform in which the game or virtual store is created. In these scenarios, safeguards should be put in place to ensure transparency related to the sharing of user data. In fact, state privacy laws like the CCPA requires that businesses must provide consumers with the right to know what personal information is sold and shared and to whom.[5] To mitigate risk, organizations should be transparent with its users on how their data is being leveraged for artificial intelligence within the metaverse.

C. Updates to the AI System

The effectiveness of an AI system is reliant on its ability to determine outcomes and make decisions based on the most current available information. Accordingly, data sets must regularly be refreshed. However, there are certain instances where this constant collection and use of information for the purpose of updating an AI system may encounter compliance issues with privacy laws.

One scenario involves scientific analysis or research. For instance, research into predictive analytics for user behavior analysis, machine learning for avatar personalization, or natural language processing for conversational AI agents may involve data sets that could incorporate personal information. Here, some privacy laws like the CCPA impose certain rules regarding information used for research purposes. Particularly:

> "Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be: (1) Compatible with the business purpose for which the personal information was collected . . . (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer,

4 Cal. Civ. Code § 1798.100(a)(1).

5 Cal. Civ. Code § 1798.115.

> by a business . . . (7) Used solely for research purposes that are compatible with the context in which the personal information was collected."[6]

Given the immense amounts of data ingested by AI training and sourced internationally, complying with requirements such as that of the CCPA may be challenging. To train AI in compliance with legal requirements for certain scientific research projects, may entail using data specifically obtained and labeled as research data. Such a process would involve giving individuals notifications and obtaining specific consents that are specifically tailored for a given research project.

05
ALGORITHMIC AND AUTOMATED DECISION-MAKING BIAS

The use of AI in the metaverse may inherently create user profiles on which certain decisions may be based. Organizations leveraging AI in this space would need to be mindful that profiles created by unverified and widely sourced information are not used to generate decisions that may negatively impact or be biased towards a certain consumer or demographic, particularly if the decision making is automated. This may be problematic where AI algorithms used in the metaverse may perpetuate biases based on the data they were trained on, leading to discriminatory outcomes and experiences for certain users. The inner workings of AI systems in the metaverse can be opaque, making it difficult for users to understand how decisions are being made and what data is being used.

States have expanded consumer rights to include giving consumers certain rights in connection with automated decision making, particularly if it produces a legal effect or significantly affect the individual. Under the CCPA, certain information used to build consumer profiles must be disclosed and may be subject to a right of opt-out for automated decisions. Additionally, the CPRA added a new definition of "profiling," giving consumers opt-out rights with respect to businesses' use of "automated decision-making technology," which includes profiling consumers based on their "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[7]

In addition, organizations that use AI to make automated decisions about consumers face another challenge – explaining how the AI works. This is a very difficult task given the "black-box" nature of predictive AI algorithms. The CPRA charges the California Privacy Protection Agency ("CPPA") with adopting regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology,"[8] including providing meaningful information about the logic of the decision and the likely outcome with respect to the consumer. While such guidance has yet to be issued, organizations contemplating the use of AI in the metaverse should bear in mind the potential rights of consumers that state privacy laws may impose and consider how the AI system may be able to practically produce supporting evidence of its automated decision regarding a metaverse consumer.

06
CYBERSECURITY THREATS

The metaverse is susceptible to various cybersecurity threats such as hacking, malware, and data breaches, that puts user data at risk. Personal data of users can be collected, shared, and exploited by metaverse operators, AI algorithms and other users, creating the risk of identity theft, fraud, and privacy violations.

Security breaches may pose a challenge to organizations leveraging AI in the metaverse because such incidents may require data breach notifications depending on the scope and type of data impacted. As summarized by the International Association of Privacy Professionals ("IAPP"), "U.S. data breach notification laws vary across all 50 states and U.S. territories. Each law must be applied to every factual scenario to determine if a notification requirement is triggered."[9] Given that PII may be gathered in large volumes in order to train AI systems, the impacted population may be quite significant.

6 Cal. Civ. Code § 1798.140(ab).

7 Cal. Civ. Code § 1798.140(z).

8 Cal. Civ. Code § 1798.185(a)(16).

9 https://iapp.org/resources/article/state-data-breach-notification-chart/.

Furthermore, how AI may be used by various organizations in the metaverse is still unknown. Should security incidents occur, certain industries may require compliance with specific data breach notification obligations. For example, the Office of the Comptroller of the Currency ("OCC"), Treasury, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation ("FDIC") issued a final rule that requires a banking organization to notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident," and under certain circumstances, notify each affecting banking organization customer.[10] The practical exercise of identifying impacted consumers may be challenging given that the volume of consumers could be significant.

To mitigate cybersecurity threats, a combination of technical and non-technical measures may be helpful, including: (i) ensuring that personal data used to train and operate AI systems is properly secured and protected from unauthorized access, theft, and misuse, (ii) providing increased human oversight and intervention to help detect and address cybersecurity threats associated with AI systems in the metaverse, and (iii) conducting regular security audits.

In January 2023, the National Institute of Standards and Technology ("NIST") released the NIST AI Risk Management Framework ("AI RMF")[11] to better manage risks to individuals, organizations, and society associated with artificial intelligence. Organizations looking to leverage AI in the metaverse should consider reviewing the AI RMF for recommendations on how to address, document, and manage AI risks and potential negative impacts effectively in order to establish more trustworthy AI systems.

07
REGULATION

The use of AI in the metaverse raises questions about jurisdiction, liability and accountability, and the need for clear, comprehensive regulation. Given the potentially vast scope of the use of AI in the metaverse and how its use may cross borders, different countries and regions will have different approaches to its regulation.

In the U.S. alone, numerous pieces of legislation related to artificial intelligence were introduced and enacted, having been prompted by concerns about potential misuse or unintended consequences of AI.[12] Recently, U.S. Representative Ted Lieu used artificial intelligence to draft the first AI-written bill for Congress,[13] signaling that AI is a current national issue. The development of AI in the metaverse is also likely to involve a range of stakeholders, including technology companies, governments, academic institutions, and public interest organizations. Regulation may also be influenced by broader international trends and agreements, such as the United Nations' discussions on responsible uses of AI[14] and the development of a global regulatory framework for AI.[15] The regulatory proposal aims to "provide AI developers, deployers and users with clear requirements and obligations regarding specific uses of AI. At the same time, the proposal seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises ("SMEs")."[16] As it stands, existing regulatory frameworks such as the CCPA, the CPRA, and the European Union's General Data Protection Regulation ("GDPR")[17] covering technology and data privacy may be used to regulate AI in the metaverse in the interim.

10 https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

11 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

12 https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence.

13 https://www.msnbc.com/the-reidout/reidout-blog/ted-lieu-chatgpt-ai-bill-congress-rcna67944.

14 https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence.

15 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

16 *Id*.

17 https://gdpr-info.eu/.

08
CONCLUSION

The convergence of artificial intelligence and the metaverse opens up incredible possibilities for advancement in innovation, social engagement, education, and global connectivity. However, with such progress, we must also consider the privacy and cybersecurity implications in order to mitigate risk and take thoughtful and deliberate steps toward protecting individuals and organizations in the metaverse while leveraging artificial intelligence.

> *In the U.S. alone, numerous pieces of legislation related to artificial intelligence were introduced and enacted, having been prompted by concerns about potential misuse or unintended consequences of AI*

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL