THE MATRIX OF PRIVACY: DATA INFRASTRUCTURE IN THE AI-POWERED METAVERSE

LEON ANIDJAR†

NIZAN GESLEVICH PACKIN††

ARGYRI PANEZI†††

ABSTRACT

How realistic is the idea of an artificial intelligence-assisted, decentralized and privacy-enhancing future generation of the World Wide Web? Could data governance and other legal tools currently employed to address the various information violations of Web2 – often in an insufficient way – help tackle the new privacy challenges that Web3 brings about? These central questions set the stage for this Article's inquiry: how do we (re-) conceptualize privacy challenges in Web3, including in immersive digital spaces, and what is referred to by some as the metaverse? The Article begins by describing such immersive virtual spaces as well as their technological foundation. It explains what privacy concerns and risks might stem from the vast amount of data generated, gathered, and exchanged in our increasingly artificial intelligence-based immersive, digital world. Most importantly, the Article argues that in Web3, data has an evolved role; it is not only a valuable resource as understood in Web1 and Web2, but it is the infrastructure itself. Building on these notions, the Article introduces the multidimensional conceptualization of how data exchanges would occur in the metaverse, by distinguishing between three levels of analysis: micro, macro, and meso. Drawing upon ideas from the Complex System Theory, we examine how information laws and artificial intelligence-related policies and regulations address privacy challenges in each level of data relationship. Finally, we propose a market-based solution that calls lawmakers to impose privacy mandatory disclosure obligations concerning compliance with data protection regulation and the use of AI as well as complementary liability regimes. This will motivate metaverse entities to self-regulate their AI infrastructures and ensure meaningful privacy protection.

TABLE OF CONTENTS

THE MATRIX OF PRIVACY: DATA INFRASTRUCTURE IN THE AI-POWERED METAVERSE

INTRODUCTION

In early February of 2023, Twitch star QTCinderella found herself trapped in a nightmare that she could not wake up from, as it was very much a reality – her likeness was featured in widely distributed deepfake pornographic video.[1] She has not been the only one. In recent years, cases of artificial intelligence (AI) and machine learning (ML) –assisted deepfake porn, in which images of unaware individuals – including celebrities like Scarlett Johansson[2] – are pasted into adult videos, have demonstrated how cutting-edge technologies are used to violate privacy and autonomy in the World Wide Web (the Web) and its developing immersive digital spaces, illustrating new challenges.[3] But some of these challenges are, to some extent, intensified versions of issues that commentators and policymakers have been concerned with since the early 2000's. For example, long before deepfake porn, Facemash, the predecessor of Facebook, was a website that invited users to compare side-by-side photos of classmates of the site's creators – Mark Zuckerberg and friends. The website was also allegedly the reason its creators almost got expelled from Harvard, presumably violating copyright law – by using students' images – and infringing upon students' right of privacy.[4] Yet, in the transition from a world dominated by tech giants and social media platforms to an immersive, multi-dimensional one – with more than one trillion uniform resource locators (URLs)[5] – addressing such challenges has become much more complicated.

† Leon Anidjar is an Assistant Professor in Business Law at IE Law School–IE University, a doctoral candidate at the Strategic Management & Entrepreneurship Department at the Rotterdam School of Management of Erasmus University, and Affiliated Research Associate at the European Banking Institute (EBI).

†† Nizan Geslevich Packin is a Professor of Law at Baruch College, City University of New York, a Senior Lecturer at the Haifa University Faculty of Law, a Fellow at the Yale Cyber Leadership Forum, and an Affiliated Faculty at Indiana University Bloomington's Program on Cybersecurity.

††† Argyri Panezi is a Canada Research Chair in Digital Information Law and Policy and Assistant Professor at the Faculty of Law of the University of New Brunswick, and a Research Fellow of the Digital Civil Society Lab at Stanford University's Center on Philanthropy and Civil Society.

The Article benefitted from valuable comments from participants at the IE Law School's Faculty Seminar and NYU School of Law's Privacy Research Group at the Information Law Institute (ILI). The authors acknowledge the outstanding research assistance of Martín Villegas, Daniella Maria Guevara and Faridi Dacasa.

[1] Andrew Court, *Twitch star QTCinderella's deepfake porn nightmare: 'F–k the internet',* New York Post (Feb. 6, 2023), https://nypost.com/2023/02/06/twitch-star-tearfully-reveals-shes-victim-of-deepfake-porn-f-k-the-internet/

[2] *Id*.

[3] For more on deepfakes and porn *see e.g.* Regina Rini & Leah Cohen, *Deepfakes, Deep Harms,* 22 J. Ethics & Soc. Phil. 143 (2022)*;* Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* , 107 Cal. L. Rev. 1753 (2019); Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions,* 78 Md. L. Rev. 892 (2019); Lauren Henry Scholz*, Private Rights of Action in Privacy Law,* 63 Wm. & Mary L. Rev. 1639, 1670 (2022).

[4] Katharine A. Kaplan, *Facemash Creator Survives Ad Board,* The Harvard Crimson (Nov. 19, 2003), https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/

[5] Mark van Rijmenam, Step into the Metaverse: How the Immersive Internet Will Unlock a Trillion-Dollar Social Economy 1 (2022).

In legal literature and social studies, the development of the Web is commonly described in three stages.[6] In the early stages of the Web – referred to herein as Web1 – individuals were able to disseminate information statically by providing read-only content, produced by a limited number of editors, that did not enable user interaction.[7] Site designers had to obtain access to a server and write complicated code to provide content to users,[8] and users were only able to consume content and could not contribute to its creation.[9] E-commerce was a part of Web1, also known as the "static web," as it allowed for the sale of products and services online, and was one of the main things that the web was used for.[10] But Web1's online shopping did not look like e-commerce does in the 2020's, as the majority of transactions were still conducted in-person or over the phone. Moreover, the process of purchasing goods and services online was often cumbersome and required users to fill-out lengthy forms and wait for confirmations before completing transactions. Likewise, most Web1websites could not be updated in real-time and did not allow for user input; there was little use of multimedia, such as videos and animations, and navigation was tricky due to the lack of standardized conventions and technologies.[11] However, Web1 did lay the foundation for the development of our modern Internet, and paved the way for the emergence of a more developed Web version – referred to herein as Web2 – which introduced greater interactivity and collaboration.[12] Having adopted an "architecture of participation," Web2 enables users, programmers, service providers, and organizations to contribute content.[13] It addressed the flows of Web1 by replacing the read-only mode of content with a read-and-write version that allows users to view content and contribute to its distribution.[14] Some argue that this new era has officially gone mainstream in 2005, with the launch of YouTube.[15] This period, the era of dynamic content, was marked by the rise of social media networks and users' ability to interact with webpages and each other,[16] largely due to Section 230 of the Communications

[6] *Id*. at 1–8.

[7] Anne Helmond, *A Historiography of the Hyperlink: Periodizing the Web Through the Changing Role of the Hyperlink*, The Sage Handbook of Web History 227, 228–229 (Niels Brügger and Ian Milligan eds., 2019).

[8] Vivek Madurai, *Web Evolution from 1.0 to 3.0,* Medium (February 17, 2018), https://medium.com/@vivekmadurai/web-evolution-from-1-0-to-3-0-e84f2c06739.

[9] Graham Cormode and Balachander Krishnamurthy, *Key Differences between Web1 and Web2*., 13(6) First Monday (2008), https://doi.org/10.5210/fm.v13i6.2125.

[10] Richard W. Fox, *The Return of "Voodoo Information": A Call to Resist A Heightened Authentication Standard for Evidence Derived from Social Networking Websites*, 62 Cath. U. L. Rev. 197, 224 (2012) (articulating that "[w]ebsite content refers to what Internet experts have defined as "Web 1.0.").

[11] Id.

[12] Tim O'Reilly, *What is Web 2.0: Designed Patterns and Business Models for the Next Generation of Software*, O'REILLY (Sept. 30, 2005), http:// oreilly.com/web2/archive/what-is-web-20.html (creating the terms Web 1.0 and Web 2.0 to explain and account for the changes made to the web).

[13] Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html;

[14] *Web 1.0, Web 2.0, and Web 3.0 with their Difference*, GeeksforGeeks (July 1, 2022), https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/.

[15] Dan Ashmore and Farran Powell, *A Brief History of Web 3.0,* Forbes (Aug. 26, 2022), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-web-3-0/.

[16] *Id*.

Decency Act (CDA),[17] a unique law,[18] which provides immunity from liability for online service providers for content created by third parties.[19] The section was enacted in 1996 – a time when Web1 was in its infancy – and reflects the strong U.S. bias towards free speech over other values.[20] It had a significant impact on the development of the internet,[21] enabling online service providers to host a wide range of user-generated content (UGC) without fearing legal liability, provided that they do not create or develop the content themselves.[22] Section 230's broad protections have enabled tech companies to become central features of the modern internet,[23] facilitating UGC,[24] which gave birth to modern advertising and enabled the creation of consumer-targeting practices.[25] Indeed, Web2 platforms made consumers become "prosumers," a hybrid of consumers and producers,[26] whose participation shapes the characteristics of the internet.[27] But Web2 also represents an era of closed platforms where users cannot move their content from one platform to others, as most are not based on interoperability.[28] Moreover, each platform's business model relies on users' exclusive use and monetization of content,[29] which is less ideal in terms of market

[17] 47 U.S.C. § 230.

[18] *See e.g.,* Eric Goldman, *The Third Wave of Internet Exceptionalism*, Tech & Mktg. L. Blog (Mar. 11, 2009), https://bit.ly/2KGhOkP; Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 Berkeley Tech. L.J. 1505, 1511-12 (2015) (comparing standards of liability for defamation).

[19] *See e.g.,* Michal Lavi*, Publish, Share, Re-Tweet, and Repeat*, 54 U. Mich. J. L. Ref. 441, 446 (2021).

[20] *See* Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 Notre Dame L. Rev. REFLECTION 33 (2019); Michal Lavi, *Do Platforms Kill?,* 43 Harv. J.L. & Pub. Pol'y 477, 512 (2020). When enacted conservative members of congress were afraid that intermediaries would not exercise editorial control. *See* Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas,* 63 U. Miam L. Rev. 137, 148 (2008) (describing concerns that entities would have "a strong incentive to never exercise editorial control," but also that they "would unjustifiably over-censor user content. ")

[21] *See e.g*. Jeff Kosseff, The Twenty-Six Words that Created the internet 77–78 (2019).

[22] Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It*, 23 Berkeley Tech. L.J. 583, 585 (2008) ("Almost uniformly, courts have interpreted § 230's safe harbor broadly.")

[23] *See generally* Anupam Chander, *How Law Made Silicon Valley*, 63 Emory L. J. 639 (2014).

[24] *See* Abbey Stemler, *The Myth of the Sharing Economy and Its Implications for Regulating Innovation*, 67 Emory L.J. 197, 216 (2017) (describing how the section has been very broadly interpreted).

[25] In *Gonzalez v. Google*, the U.S. Supreme Court will consider Section 230's scope in connection with targeting certain content to users based on their online activities. Lydia Wheeler and Kimberly Strawbridge Robinson, *Top Five US Supreme Court Cases to Watch in the New Year*, Bloomberg, (Jan. 3, 2023), https://news.bloomberglaw.com/us-law-week/top-five-us-supreme-court-cases-to-watch-in-the-new-year.

[26] Veronica Barassi and Emiliano Treré, *Does Web 3.0 Come After Web 2.0? Deconstructing Theoretical Assumptions Through Practice*, 14(8) New Media and Society 1269, 1271–1272 (2012).

[27] Margaret Chon, *The Romantic Collective Author*, 14 Vand. J. Ent. & Tech. L. 829, 849 (2012) (noting that Web 2.0 stands "in contrast to Web 1.0, which consists mostly of websites that do not allow or promote interactivity of content creation."); Brian Getting, *Basic Definitions: Web 1.0, Web 2.0, Web 3.0,* Prac. eCommerce (Apr. 18, 2007), http://www.practicalecommerce.com/articles/464/basic-definitions-web-10-web-20-web-30; Ripple Venture, *The Benefits and Drawbacks of Web 2*, Medium (December 16, 2021), https://medium.com/rippleventures/the-benefits-and-drawbacks-of-web-2-part-2-of-7-90f792165542.

[28] Interoperability refers to different web-browsers' or devices' ability to access and display content consistently and correctly. Some view it as a desirable feature as it allows users to use a wide range of resources and services without being limited by devices or software' compatibility. *See e.g.* Gabriel Nicholas, *Interoperability and Portability in the Wild: Lessons from the Data Sharing Practitioners Workshop,* The Engelberg Center, NYU (2021), https://www.law.nyu.edu/sites/default/files/interoperability_and_portability_in_the_wild_202104.pdf.

[29] van Rijmenam, *supra* note 5 at 5.

competition.[30] Similarly, Web2 – contrary to the vision of creating an open, free network – is characterized by tech giants that charge users for distributing and accessing content,[31] and the 'data as a payment model,' which makes users sacrifice their privacy in order to enjoy free services in exchange for their data.[32] And while some critics have argued that these practices are designed to work against consumers' best interests,[33] and exploit them,[34] others associated the absence of rational consumer decision-making with the low value consumers place on privacy.[35] But despite Web2's data management and privacy-related shortcomings the Web keeps developing, and with more than 5 billion regular users – about 63% of the global population[36] – many wonder how its next iteration (referred to herein as Web3) would be. Arguably designed to address Web2's failings, Web3 (or Web 3.0, Semantic Web, Web of Data, or Web of Intelligence[37]) has been used to describe a futuristic Web in which the

[30] Peter K. Yu, *Data Producer's Right and the Protection of Machine-Generated Data*, 93 Tul. L. Rev. 859, 889 (2019) (noting that "if we are to maximize our ability to undertake big data analyses, such analyses may require greater sharing of data--which, in turn, calls for greater data portability and interoperability."); Peter K. Yu, *The Algorithmic Divide and Equality in the Age of Artificial Intelligence*, 72 Fla. L. Rev. 331, 384 (2020) (explaining that "the better coordinated the data usage is, the more benefits []. . . competition will provide.").

[31] Jad Esber and Scott Duke Kominers, *Why Build in Web3*, Harvard Business Review (May 16, 2022), https://hbr.org/2022/05/why-build-in-web3(in such "business models, locking in users and their data is a key.").

[32] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 Colum. L. Rev. 1369, 1384–1385 (2017) (under such a payment model "companies can monitor a consumer's habits, including Internet browsing on third-party websites, not only from the consumer's direct use of the product but also by using cookies")

[33] Gabe Maldoff & Omer Tene, *The Costs of Not Using Data: Balancing Privacy and the Perils of Inaction,* 15 J.L. Econ. & Pol'y 41, 43 (2019) (citing "the abject market failures, information asymmetries, and imbalance of power between individuals and firms" as problems that lead consumers to "resign."); Elizabeth M. Renieris & Dazza Greenwood, *Do We Really Want to "Sell" Ourselves? The Risks of a Property Law Paradigm for Personal Data Ownership,* MEDIUM (Sept. 23, 2018), https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa.

[34] Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Annenberg School for Communication, University of Pennsylvania (June 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[35] *See e.g.* Gordon Hull, *Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data*, 17 Ethics & Info. Tech. 89 (2014); Noam Kolt, *Return on Data: Personalizing Consumer Guidance in Data Exchanges*, 38 Yale L. & Pol'y Rev. 77 (2019) (suggesting that privacy concerns should not be viewed in isolation, but as part of Return on Data); *Survey Shows Consumers Very Willing To Trade Personal Data for Financial Benefits,* PRNewswire (Aug. 5, 2020), https://www.prnewswire.com/news-releases/survey-shows-consumers-very-willing-to-trade-personal-data-for-financial-benefits-301106196.html (finding that 50% of consumers try to limit data tracking and protect privacy). Some argue that consumers make irrational decisions, as they do not read privacy notices, and do not understand them if they do read. Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure*, 159 U. Pa. L. Rev. 647, 665 (2011). One possible reason for this is lack of time. Keith Wagstaff, *You'd Need 76 Days to Read All Your Privacy Policies Each Year*, TIME (Mar. 6, 2012), http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/.

[36] *See* Ashmore and Powell, *supra note* 15.

[37] *See e.g. Web 1.0 vs Web 2.0 vs Web 3.0 vs Web 4.0 vs Web 5.0 - A Bird's Eye on the Evolution and Definition,* FLAT WORLD BUS., https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition*;* Aghaei et.al, *3:1 Intl' J. of Web & Semantic Technology* (IJWesT), (Jan. 2012), http://airccse.org/journal/ijwest/papers/3112ijwest01.pdf.; Norasak Suphakorntanakit, Web 3.0, (2008), http://webuser.hs-furtwangen.de/~heindl/ebte-08ssweb-20-Suphakorntanakit.pdf.

internet would be more intelligent, semantically rich, and interconnected.[38] As such, some envision it to offer a decentralized digital experience that would allow users to take back control over their data by operating without intermediaries thereby enhancing their autonomy and privacy. But "[b]ecause it remains a collection of ideas more than anything else, it's challenging to nail down a precise definition of Web3."[39] Despite Web3's unclear definition, one assumption that this Article focuses on is that it would be powered by advanced technologies that include AI, ML, natural language processing (NLP), and "smart" agents performing tasks on behalf of users, enabling it to organize, store, access, and supplement unprecedented amounts of data online. Moreover, these technologies would likely use data as infrastructure,[40] which would presumably allow users to access more relevant and personalized information, and enable the automated creation of intelligent and interactive applications and services. How would this evolution develop? Some commentators argue that the answer is blockchain technology, which functions many Web3 applications.[41] Among the applications they refer to is the metaverse,[42] which promises a new three-dimensional, immersive experience of the Web and brings the physical and digital worlds closer, using crypto assets, such as non-fungible tokens (NFTs).[43] Additionally, decentralized ledger

[38] Sean B. Palmer, *The Semantic Web: An Introduction*, (2001), http://infomesh.net/2001/swintro/; Ossi Nykänen, *Semantic Web: Definition*, (2003), http://www.w3c.tut.fi/talks/2003/0331umediaon/slide6-0.html.

[39] *Id*.

[40] Zoe Niesel, *Machine Learning and the New Civil Procedure*, 73 SMU L. Rev. 493, 496 (2020) (describing "Web 3.0 technologies--such as machine learning, AI, and human-computer interfacing"); Julia Y. Lee, *Trust and Social Commerce*, 77 U. Pitt. L. Rev. 137, 181 (2015) (explaining that "[s]ome have begun referring to Web 3.0, a third generation of the Web, characterized by use of semantic web technologies, natural language processing, machine learning, and artificial intelligence technologies."); Zoe Niesel, *#personaljurisdiction: A New Age of Internet Contacts*, 94 Ind. L.J. 103, 137 (2019) (describing the goal of Web3 applications as "immersion with an ecosystem that understands itself and is able to freely correct and publish information through the use of artificial intelligence. Additionally, users will be able to publish their own content and services by interacting with applications built by companies and other users.").

[41] Such commentators explain that the seeds of Web 3 were planted in 2009 when Bitcoin was launched. *See e.g.* Balázs Bodó and Alexandra Giannopoulou*, The Logics of Technology Decentralization – The Case of Distributed Ledger Technologies,* in Blockchain and Web 3.0: Social, Economic, and Technological Challenges 114(Massimo Ragnedda and Giuseppe Destefanis eds., 2019) ("The Nakamoto paper describes a technology that can be applied without needing established, centralized, and trusted intermediaries."); Mary C. Lacity and Steven C. Lupien, Blockchain Fundamentals for Web 3.0 99–152 (2022).

[42] Jon M. Garon, *Legal Implications of a Ubiquitous Metaverse and a Web3 Future* 11 (January 3, 2022), https://ssrn.com/abstract=4002551 (describing the Metaverse as "an immersive virtual world serving as the locus for all forms of work, education, and entertainment experiences."). For more *see* Section II.

[43] Those supporting this approach believe NFTs will be vital for Web3 for four reasons. First, NFTs allow for the creation of unique digital assets that could revolutionize ownership. *See e.g. Hermes Int'l v. Rothschild,* No. 22-CV-384 (JSR), 2022 WL 1564597, at 1 (S.D.N.Y. May 18, 2022) (NFTs "are units of data stored on a blockchain that are created to transfer ownership of either physical things or digital media"). Second, NFTs can help create an artificial limited supply of digital assets, creating a scarcity like effect. *See* Amy Adler & Jeanne C. Fromer, *Memes on Memes and the New Creativity*, 97 N.Y.U. L. Rev. 453, 562 (2022) (criticizing this effect). Third, NFTs have the potential to create new forms of revenue for creators of content. *See e.g.,* Brian L. Frye*, After Copyright: Pwning NFTs in a Clout Economy,* 45 Colum. J.L. & Arts 341 (2022). Lastly, NFTs can help with decentralized applications (dApps). *See* Kimberly A. Houser & John T. Holden, *Navigating the Non-Fungible Token*, 2022 Utah L. Rev. 891, 900 (2022) (noting that the Ethereum blockchain "functionality enabled NFT marketplaces to run. . . guaranteeing security and anonymity without centralized oversight.")

technology (DLT), which includes blockchain,[44] is presumably fundamental in operating new types of communities and even new and innovative business models,[45] such as decentralized autonomous organizations (DAOs).[46] But not everyone agrees with this approach, as some believe that while there may be an overlap between the next Web iteration and blockchain technology, Web3 could exist without blockchain and crypto.[47]

How realistic is the idea of an AI-assisted, decentralized and privacy-enhancing future generation of the Web? Could data governance and other legal tools currently employed to address the various information and privacy challenges of Web2 – often in an insufficient way – help tackle the challenges that Web3 brings about? These central questions set the stage for this Article's inquiry: how do we (re-) conceptualize privacy challenges in the AI-assisted Web3, including in immersive digital spaces, and what is referred to as the metaverse? Indeed, despite the notable hype around the metaverse, it is not yet clear whether it will be the centerpiece application of Web3, or how revolutionary and popular it will be.[48] It is not even clear whether there is/will be only one or many metaverses. Amidst uncertainty, but also rapid technological evolution, policymakers must act fast to understand and address the possible risks associated with the unprecedented amount of data that would be exchanged in and used in Web3. Attempting to help with that, this Article focuses on the metaverse, as a potential Web3-application and describes possible privacy challenges and data governance issues, by considering two different starting focal points.[49] The first focal point perceives the metaverse as an extension of Web2 applications in which each tech giant develops its own virtual space that is fully controlled and manipulated by the relevant entity.[50] Indeed, in that situation, according to a perspective that we define as the *private view,* we assume that each tech giant would develop an infrastructure that allows it to offer a customized to its own

[44] Blockchain, a secure and transparent technology is just one subcategory of DLT technology. *See Distributed Ledger Technology System - A Conceptual Framework,* the Cambridge Centre for Alternative Finance (Aug. 2018), https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/. Bitcoin, the first and most known cryptocurrency, utilizes blockchain technology, but there are not too many workable use-cases for blockchain technology beyond cryptocurrencies. *See e.g.* Isabelle Bousquette, *Blockchain Fails to Gain Traction in the Enterprise,* WSJ (Dec. 15, 2022), https://www.wsj.com/articles/blockchain-fails-to-gain-traction-in-the-enterprise-11671057528 (describing blockchain projects that were abandoned or move slowly.).

[45] *See* Garon, *supra* note 42.

[46] For discussions on what are DAOs and related legal challenges *see* Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4 Stan. J. Blockchain L. & Pol'y 152 (2021); Yuliya Guseva, *The Sec, Digital Assets, and Game Theory*, 46 J. Corp. L. 629 (2021); Carla L. Reyes, Nizan Geslevich Packin & Benjamin P. Edwards, *Distributed Governance*, 59 Wm. & Mary L. Rev. Online 1 (2017).

[47] *See e.g.*, Ryan Browne, *Web Inventor Tim Berners-Lee Wants Us To 'Ignore' Web3: 'Web3 Is Not The Web At All',* CNBC (Nov. 4 2022), https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html (noting the Web inventor does not view blockchain as a viable solution for its next version).

[48] Matthew Ball, The Metaverse: And How It Will Revolutionize Everything 23 (2022) ("debate over what the Metaverse is, how significant it might be, when it will arrive, how it will work, and the technological advances that will be required is exactly what produces the opportunity for widespread disruption.")

[49] François Candelon, Michael G. Jacobides, Maxime Courtaux, and Gabriel Nahas, *Four Visions of the Metaverse*, BCG Henderson Institute (Oct. 14, 2022), https://www.bcg.com/publications/2022/four-control-models-of-metaverse.

[50] *Id*.

platform experience.[51] Under this possibility, the Article claims that with some necessary adjustments, current legal tools, which mainly include privacy and antitrust laws – although not always sufficient even in Web2 – could arguably help address many of the new challenges. However, since the extraordinary costs of creating state-of-the-art hardware will be a market barrier for other companies, lawmakers should be mindful of the fact that tech companies that are early developers of this space have an incentive to ensure that this ecosystem develops into a limited market controlled by a small number of players.[52] To address the challenges associated with the one world of the metaverse, scholars have already started researching how to modify traditional branches of law.[53] For example, Jon Garon surveyed laws related to the metaverse operations and activities, such as gambling, money transfer, securities, privacy, copyrights, data governance, and cybersecurity laws.[54] He concluded that technologists, practitioners, and regulators must calibrate traditional doctrines to solve the metaverse's privacy problems and unleash its potential social benefit.[55]

Differently, the second focal point assumes that the metaverse will become a fully decentralized virtual space not exclusively controlled by any business entity.[56] According to a perspective that we define as the *public view*, which is the scenario for the development and popularity of the metaverse, we assume that the metaverse will include multiple virtual platforms creating soft barriers to retaining users. It would allow a shared ecosystem of providers, including content producers and maybe also DLT developers, who rely on open-source technology,[57] and foster a more dynamic and pluralistic marketplace of participants. Such an open metaverse will likely comprise "a collection of interconnected worlds in which users have permission-less access to contribute to the environment."[58] It is based on the idea of interoperability that allows parties to exchange meaningful data without centralized involvement. And if this public view of the metaverse will materialize, lawmakers would need to create a unique policy to mitigate privacy and data management concerns outside the boundaries of the Web2 era, as this Article suggests. Finally, if Web3 ends up not proving very different from Web2, this Article's framework can still serve as a useful benchmark in assessing the application of existing laws to the metaverse context.

The Article is structured as follows. Part I describes the metaverse and discusses its technological foundation and associated privacy concerns. It explains how privacy risks stem from the vast amount of data generated, gathered, and exchanged in the metaverse. Most

[51] For more on the antitrust aspects of such scenarios, *see* Thibault Schrepel, *The Complex Relationship between Web2 Giants and Web3 Projects* (Jan. 10, 2023), Amsterdam Law & Technology Institute Working, https://ssrn.com/abstract=4284597.

[52] *Id*.

[53] Garon, *supra* note 42; Levan Nanobashvili, *If the Metaverse is Built, will Copyright Challenges Come?,* 21 UIC Rev. Intell. Prop. L. 215 (2022).

[54] Garon, *Id*. parts 4 & 5.

[55] *Id*. at 32–35.

[56] Candelon, Jacobides, Courtaux, & Nahas*, supra* note 49.

[57] *Id.*

[58] Andrew Park et al., *Interoperability: Our Exciting and Terrifying Web3 Future*, Business Horizons 18 (2022).

importantly, it argues that in the metaverse, data has an evolved role; it is no longer a valuable resource as understood in Web1 and Web2, since in Web3, data is the infrastructure itself, autonomously and outmodedly utilized by AI and ML applications. Part II describes the potential privacy challenges in metaverse, illustrating them in three different levels applicable to the individual user. Part III introduces the multidimensional conceptualization of data exchanges in the metaverse, which are traced at the following three levels, micro, macro, and meso. *First,* at the micro-level, Complex System Theory is employed to describe data exchanges and what it means for data flows to be non-linear and dynamic, unlimited in space and in time between players interacting on different platforms. Current privacy laws, for instance privacy torts, will be applicable, yet as we argue not sufficient to address privacy violations at the micro-level. *Second*, at the macro-level, current individualistic approaches to privacy are critiqued as less relevant for analyzing the metaverse's complex data relations. *Third*, at the meso-level, analysis of existing legal tools of data governance are presented as arguably relevant, unlike at the micro and macro levels, where we argue that developing new understandings of privacy and data governance and a unique set of laws to enhance privacy is essential. Part IV continues by exploring possible solutions to privacy challenges in the micro-level of the metaverse. To mitigate the complexity of data exchanges and relationships, and their consequences to privacy protection, this part explores the potential and overall benefits of a market for privacy mandatory disclosure obligations. Finally, the Article concludes with insights regarding users' privacy rights and future interactions on Web3.

I. THE TECHNOLOGICAL FOUNDATION OF THE IMMERSIVE VIRTUAL SPACE: LAYERS OF ACTIVITIES, PLAYERS, AND APPLICATIONS

A presumably natural application of Web3, the metaverse is a virtual shared space, which could not have existed in Web1 or Web2, given their very distinct characteristics.[59] The notion of the metaverse can only be created by the convergence of virtually enhanced physical reality and physically persistent virtual space, using cutting-edge technologies as further described below. In its essence, the term 'metaverse' is frequently used to describe "a

[59] Table 1 – Key differences between Web1.0, 2.0, and 3.0

Category	Web1	Web2	Web3
Concept	'Read-only' web	'Read-write' web	'Read-write-execute' web
Framework	Static content	Dynamic content	Personalized content via AI / ML
Function	Content published by companies and utilized by users (one-way publishing)	Allow users to post content while companies provide a platform for sharing knowledge	Platforms, applications, and networks, allow user interactions without the need for mediating entities via advanced technology
Goal	Information Sharing	Interaction	Immersion

fully realized digital world that exists beyond the one in which we live."[60] It was coined by Neal Stephenson in his 1992 science fiction novel "Snow Crash,"[61] explored by Ernest Cline in his novel "Ready Player One,"[62] and discussed in science-fiction circles.[63] Finally, technology advances, and the pandemic, which shifted life to online-everything, got the metaverse more attention.[64] The vision for the metaverse is a fully immersive virtual world that is seamlessly integrated with the real world, where users can interact with each other and with virtual objects and environments in real-time. But while Web3 could potentially be significant in achieving the potential of the metaverse, Matthew Ball, the author of '*The Metaverse: And How It Will Revolutionize Everything,*' pointed out that there is no inherent connection between the two. They can operate independently of each other.[65] The vision associated with the metaverse is an immersive virtual world that is seamlessly integrated with the real world,[66] and could potentially provide a new platform for social interaction, education, and entertainment, thereby creating new economic opportunities.

A. Multiple Realities

In terms of what an immersive digital space looks and feels like, the metaverse can take many forms, which utilize virtual reality (VR), augmented reality (AR), and extended reality (XR). It could be a virtual world that resembles a video game, such as Roblox,[67] which has about 56.7 million daily active users,[68] with environments representing physical ones, and avatars representing users and digital objects, or XR and AR situations, where virtual elements are

[60] John Herrman and Kellen Browning, *Are We in the Metaverse Yet?,* N.Y.Times, (Oct 29, 2021), https://www.nytimes.com/2021/07/10/style/metaverse-virtual-worlds.html?action=click&pgtype=Article&state=default&module=styln-metaverse&variant=show&region=MAIN_CONTENT_1&block=storyline_levelup_swipe_recirc

[61] Kashmir Hill, *This Is Life in the Metaverse*, N.Y.Times (Oct. 7, 2022), https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html.

[62] *Id*.

[63] Madhavi Sunder, *IP3*, 59 Stan. L. Rev. 257, 307 (2006).

[64] Brian Chen, *The Tech That Will Invade Our Lives in 2022*, N.Y.Times, (Jan. 6 2022), https://www.nytimes.com/2022/01/05/technology/personaltech/tech-2022-vr-metaverse.html?action=click&pgtype=Article&state=default&module=styln-metaverse&variant=show&region=MAIN_CONTENT_1&block=storyline_levelup_swipe_recirc

[65] James Ross, *Web3 Was Meant To Be Integral To The Metaverse—It Isn't Yet,* Forbes (Jan. 5, 2023), https://www.forbes.com/sites/forbesagencycouncil/2023/01/05/web3-was-meant-to-be-integral-to-the-metaverse-it-isnt-yet/?sh=11d29417624f.

[66] Recent reports about the metaverse include information about how the VR space will now enable bringing smell and taste to users. *See* Byhaleluya Hadero, Rio Yamat And The Associated Press, *Metaverse Ventures Bring Smell And Taste To Virtual Reality At CES 2023: 'At Least You Can Feel Something'*, Fortune (Jan. 8, 2023), https://fortune.com/2023/01/08/metaverse-ventures-bring-smell-and-taste-to-virtual-reality-at-ces-2023-at-least-you-can-feel-something/.

[67] Beckett Cantley, Geoffrey Dietrich, *The Metaverse: A Virtual World with Real World Legal Consequences*, 49 Rutgers Computer & Tech. L.J. 1, 3 (2022) (defining Roblox as the "largest online game creation platform.")

[68] Sofia Pitt, *Roblox Closes Down More Than 15% After November Update Shows Slowing Growth*, CNBC (Dec. 15 2022), https://www.cnbc.com/2022/12/15/roblox-stock-sinks-after-november-update-shows-slowing-growth.html.

overlaid on top of the real world in real-time.[69] And although gaming was the initial AR application that reached a broad audience, it is not the only one.[70] The metaverse could potentially be accessed through a variety of devices, including AR glasses, and other wearable technology, and VR equipment that big tech companies have focused on in recent years. For example, Facebook, which started pursuing its interest in VR in 2014, purchased back then VR company Oculus for $2 billion, gaining the ability to track and influence behavior in both real and virtual three-dimensional environments.[71] In 2020, Facebook introduced Project Aria, a project that uses augmented reality glasses to map the world and objects within it.[72] Then, in 2021, the company's Oculus Quest 2 VR headset became extremely popular.[73] But the interest in innovative new technologies has expanded beyond mere VR to cover more broadly metaverse-related aspects and prospects, and other big tech companies have started making significant investments in the space. Wanting to create a virtual environment where people can work, play, and communicate with each other in a fully immersive manner, in 2020 Facebook renamed Oculus as 'Reality Labs' and in 2021 rebranded itself as 'Meta.'[74] In doing so, Mark Zuckerberg, Facebook's founder and CEO, has connected the new name to his strategic plan to develop a metaverse social network.[75]

An early example of a social virtual world is the platform "Second Life,"[76] which launched in 2003.[77] The platform – which very soon became less of an anomaly with other platforms offering the same concept[78] – is a massively multiplayer online virtual world that was created

[69] Many first encountered AR through the game Pokémon GO. AR technology overlays digital content on the real world. Users can view the world with digital images appearing by using devices/special glasses. *See* Mark Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. Pa. L. Rev. 1051, 1054 (2018).

[70] *Id*.

[71] Josh Constine, *Facebook's $2 Billion Acquisition of Oculus Closes, Now Official*, TECHCRUNCH (July 21, 2014, 1:04 PM PDT), https://techcrunch.com/2014/07/21/facebooks-acquisition-of-oculus-closes-now-official/

[72] *See* S.A. Applin, *Why Facebook is Using Ray-Ban to Stake a Claim to our Faces*, MIT TECH. REV. (Sept. 15, 2021), https://www.technologyreview.com/2021/09/15/1035785/why-facebook-ray-ban-stories-metaverse/

[73] Will Greenwald, *The Best VR Headsets for 2021*, PC MAG. (Oct. 21, 2021), https://www.pcmag.com/picks/the-best-vr-headsets. Zuckerberg referred to it as "an embodied Internet that you're inside of." *See* Kyle Chyka*, Facebook Wants Us to Live in the Metaverse,* NEW YORKER (Aug. 5, 2021), https://www.newyorker.com/culture/infinite-scroll/facebook-wants-us-to-live-in-the-metaverse.

[74] Sorkin, Karaian, Kessler, Merced, Hirsch and Ephrat Livni, *Could a New Name Help Facebook After All?*, N.Y. Times, (Oct. 29, 2021), https://www.nytimes.com/2021/10/29/business/dealbook/facebook-meta-rebranding.html; Shirin Ghaffary, Facebook's Name Change Plan Reflects its Real Priorities, VOX (Oct. 20, 2021, 4:45 PM EDT), https://www.vox.com/recode/2021/10/20/22737168/facebook-name-change-metaverse-zuckerberg-frances-haugen-whistleblower.

[75] *Id*. (noting the change "also comes as Zuckerberg and his company are under intense scrutiny over leaked documents that show the company was aware of the societal damage its products have caused. Some say the name change is an effort to leave behind what is wrong with Facebook without making substantial changes.")

[76] Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. Rev. 1047, 1102 (2005) (defining the platform as "a non-game open architecture virtual environment that lets users build whatever content they like").

[77] *See, e.g.,* Andrew Lavalee*, Now, Virtual Fashion*, Wall St. J., Sept. 26, 2006, at B1 (describing "the fast-growing virtual world of Second Life.").

[78] Indeed, it became clear quickly that "[t]ens of millions of people spend hours a day playing such games. . . They live in a virtual world. . .They sell land, sell their bodies, run gambling parlors, design and construct buildings, buy and spend virtual money, hack into each other's accounts to steal virtual property, and now even

and owned by its residents, who interact with each other through avatars and can create and build their own virtual world. Users can also earn and spend a virtual currency called Linden dollars, which can be exchanged for real-world currency.[79] The virtual world of Second Life is divided into parcels of land, which can be owned by users, and the game offers a wide range of activities for its users such as socializing, entertainment, and even learning and earning opportunities.[80] Users can create their own virtual items, vehicles, buildings, and even animations, and they can also buy and sell virtual goods and services.[81]

Under Zuckerberg's leadership, Meta took the Second Life concept, and upgraded it into a platform called horizon, which is designed to be "Meta's universe in the metaverse."[82] Horizon is intended to be a fully immersive virtual world in which users can freely interact in real-time.[83] They can also create their own avatars, explore virtual worlds, and partake in activities and events in which other users are participating.[84] Horizon is accessible via a VR headset, but users can also access the platform via a computer or smartphone.[85] One of the main goals of Horizon is to provide a new platform for social interaction, education, and entertainment, and create new economic opportunities, such as virtual events and concerts, and the buying and selling of virtual "real estate."[86] Big tech entities that have been working on metaverse-related technology,[87] are arguably interested in VR due to its potential to expand their power, which includes "a dominant share of biopower to achieve biosupremacy, monopolistic power over human behavior."[88] But the commercial and financial success of such entities depends on how much time consumers are willing to spend connected to immersive digital spaces, which may become more appealing in the future as VR technology

sue one another in "reality" for being defrauded in virtual transactions." George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?,* 13 Rich. J.L. & Tech. 10, 10 (2007).

[79] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency,* 4 Hastings Sci. & Tech. L.J. 159, 171 (2012).

[80] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614, 655–56 (2011) (mentioning Second Life and noting that "[w]hile nothing may ever replace a dinner at home with family and friends, social media provide other ways to converse, to play games, to pursue hobbies, to share entertainment, and to meet.")

[81] The game had reached its peak popularity in 2006-2010, but since then, its user numbers has been declining.

[82] *See* Hill, *supra* note 61.

[83] *Id*. (recapping her experiences in Horizon, the author loved "meeting people spontaneously.").

[84] Id. (indicating that "explaining the metaverse through the lens of Horizon feels akin to unpacking the potential of "the web" by surfing AOL chat rooms in the 1990s, during the days of dial-up modems.").

[85] *Id*.

[86] *Id*.

[87] Cade Metz, *Everybody Into the Metaverse! Virtual Reality Beckons Big Tech,* N.Y.Times, (Dec 30, 2021), https://www.nytimes.com/2021/12/30/technology/metaverse-virtual-reality-big-tech.html?partner=IFTTT (explaining how the biggest tech companies are joining game makers in pursuit of an immersive digital world).

[88] *See* Mason Marks, *Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior*, 55 U.C. Davis L. Rev. 513 (2021). Marks argues that "[w]hile regulators' eyes are fixed on Google and Facebook's search and advertising business, and government resources are tied up battling their armies of corporate lawyers, Google and Facebook will. . . expand their biopower, and move closer to biosupremacy, while the ongoing lawsuits create a distraction for Congress, regulators, and the public. . . If U.S. antitrust retains its focus on consumer welfare, the government will be unprepared," as the metaverse will consolidate biopower. *Id*., 572. Focusing on this, Marks suggests bridging the gap between existing antitrust doctrine and future needs. *Id.*

improves. So far, corporate efforts to advance the metaverse's popularity have not resulted in great success,[89] including its associated consumer electronics device.[90] But as the VR experience continues to improve, tech giants like Meta are also likely to attract more customers than Second Life due to their ability to utilize their existing platforms like Facebook, Instagram, and WhatsApp's advertising and commercialization-based business model, to capture the habits and needs of Generation Z.[91] Particularly, as members of Generation Z are warming up to using VR and other XR gadgets, which were a harder "sell" in the past.[92] Indeed, more than 50% of surveyed Generation Z members identify with "living online," and spend more time interacting with peers via video games (65%) than at school (64%) or work (51%),[93] and this trend is likely to continue.[94] Some of the main benefits of a VR-based metaverse are convenience and realism. If consumers enjoy living virtually from their homes, then VR will become popular.[95] The more realistic the metaverse is in allowing people to work, learn, socialize, play, and shop,[96] the longer we will use it for. Thus, designing it to be easily accessible from smart devices, to increase engagement, is key for tech giants' revenues derived from digital commerce and advertising.

Meta's immersive digital platform would compete with other tech companies' VR worlds for consumer attention and engagement. The key for each platform is to gather large amounts of user data, which is a most valuable resource, to personalize offerings using AI and ML

[89] *See* James Ross, *Web3 Was Meant To Be Integral To The Metaverse—It Isn't Yet*, Forbes (Jan. 5, 2023), (giving Decentraland as example, and how "[i]n October, the Web3 metaverse platform attracted swaths of ridicule after CoinDesk reported only 38 "daily active" users wandered its virtual land in the span of 24 hours."); Ramishah Maruf, *Virtual Reality Titan John Carmack Is Leaving Meta,* CNN (Dec. 18, 2022), https://www.cnn.com/2022/12/18/tech/meta-john-carmack-resignation/index.html (explaining that "Meta lost $9.4 billion in the first nine months of 2022 on its metaverse efforts.")

[90] Jonathan Vanian, *Metaverse Off To Ominous Start After VR Headset Sales Shrank In 2022*, CNBC (Dec. 28, 2022), https://www.cnbc.com/2022/12/28/metaverse-off-to-ominous-start-after-vr-headset-sales-shrank-in-2022.html (reporting that "[s]ales of virtual reality headsets in the U.S. declined 2% year over year to $1.1 billion as of early December" and "[w]orldwide shipments of VR headsets as well as augmented reality devices dropped more than 12% to 9.6 million in 2022.").

[91] Greg Petro, *Gen Z Set To Lead Retailers Into The Metaverse,* Forbes (May 14, 2022), https://www.forbes.com/sites/gregpetro/2022/05/14/gen-z-set-to-lead-retailers-into-the-metaverse/?sh=3307a40118ed

[92] Unlike the failure of Google Glass that was "due to the lack of clarity on why this product exists." *See* Clara Yoon, *Assumptions that led to the failure of Google Glass*, Medium (Aug. 2, 2018), https://medium.com/nyc-design/the-assumptions-that-led-to-failures-of-google-glass-8b40a07cfa1e

[93] Ellyn Briggs, *Gen Z Is Extremely Online,* MorningConsult, (Dec. 12, 2022), https://morningconsult.com/2022/12/12/gen-z-social-media-usage/

[94] Gilad Yadin, *Virtual Reality Surveillance*, 35 Cardozo Arts & Ent. L.J. 707 (2017) (claiming that "[w]e are in the midst of a virtual reality renaissance").

[95] *See e.g.* Pete Pachal, *How Smart TVs Could Help the Metaverse Crack the Mass Market*, Coinsdesk (Jan. 6, 2023), https://www.coindesk.com/web3/2023/01/06/how-smart-tvs-could-help-the-metaverse-crack-the-mass-market/(noting Web3 features are starting to appear on smart TVs and could be a game changer for consumers).

[96] *See e.g.* Samantha Kubota *Mom Goes Viral For Finding Daughter On Roblox And Telling Her To Defrost The Lasagna,* Today, (Jan. 7, 2023), https://www.today.com/parents/moms/mom-finds-daughter-roblox-rcna64740 (explaining how the mother started using the VR platform to bond with her child).

tools.[97] A carefully tailored, AI-powered virtual world may engage consumers so effectively that they will spend more time in it than on any currently existing or main platforms. Since the metaverse is meant to function as an alternate reality, consumers may never want to leave it, resulting in the creation of more user data than any of the large online platforms can currently solicit. This would result in many data management and privacy-related challenges and risks; some of which already known and relevant today, and others more unique and relevant to VR data.[98] Any company operating a VR metaverse could theoretically use its vast database to target consumers with precision and send them to virtual stores, which brands will need to rent "space" from them, in the same way they currently do in physical malls. The metaverse may become essential real estate for companies to interact with their customers, whether they are consumers or business clients. Under such a scenario, Meta or other gatekeepers, may be able to control and charge entities for access to customers more effectively than other tech company have to date,[99] potentially becoming dominant players and creating an alternate reality known as the "gatekeeper economy."[100]

B. AI Systems

The metaverse is often connected to the concept of Web3, which is characterized by the use of semantic technologies, such as NLP, AI and ML, to make the internet more intelligent and easier to use. One key area in which AI is already making a significant difference is in the creation of the metaverse. While human editing and oversight will still be necessary for many tasks in the near future, data is the driving force behind AI tools, and ML improves usage, which will make the results grow exponentially. As demonstrated in 2022 by Dall-E[101] and

[97] *See, e.g.,* Yafit Lev-Aretz, *Facebook and the Perils of a Personalized Choice Architecture*, TECHCRUNCH (Apr. 24, 2018, 3:30 PM PDT), https://techcrunch.com/2018/04/24/facebook-and-the-perils-of-a-personalized-choice-architecture/ (describing how data can help design personalized offerings). For more big data and AI *see* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671, 673-74 (2016).

[98] For a discussion of the challenges in regulating VR data *see* Yeji Kim, *Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent*, 110 Cal. L. Rev. 225, 226 (2022) (focusing on (i) the challenge of aggregate data; (ii) the challenge of highly accurate but distorted data; (iii) the challenge of subtle psychological manipulation; and (iv) the overall challenge against the GDPR).

[99] Facebook, an Information gatekeeper, already alters standards surrounding news creation, distribution and consumption. *See* SUBCOMM. ON ANTITRUST, COM. & ADMIN. L. OF THE COMM. ON THE JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 62-63 (2020).

[100] Thomas A. Lambert, *Addressing Big Tech's Market Power: A Comparative Institutional Analysis*, 75 SMU L. Rev. 73, 85–86 (2022) (noting that "three approaches--antitrust law, ex ante regulation, and continual agency oversight--have been used or proposed as means of addressing market power concerns arising from dominant digital platforms. In the United States, each of the GAFA firms is currently defending major antitrust lawsuits. In Europe, the European Commission proposed a Digital Markets Act that would impose a set of common ex ante rules on large digital platforms deemed to be economic "gatekeepers."). Likewise, gatekeepers in other related areas were also discussed in the literature. *See e.g.* Stephen Choi, *Market Lessons for Gatekeepers*, 92 Nw. U. L. Rev. 916, 934-49 (1998); Frank Partnoy, *Barbarians at the Gatekeepers?: A Proposal for A Modified Strict Liability Regime*, 79 Wash. U. L.Q. 491 (2001) (discussing law and accounting firms as gatekeepers").

[101] Cade Metz, *Meet DALL-E, the A.I. That Draws Anything at Your Command*, N.Y.Times (April 6, 2022), https://www.nytimes.com/2022/04/06/technology/openai-images-dall-e.html

ChatGPT,[102] advancements in AI have already had a significant impact on the creation of virtual work, products and environments, and much more is to come. For example, Atlas is a company that allows users to create 3D gaming, virtual work, and metaverse environments using simple language commands. It enables users to generate – by entering a few keywords – detailed, realistic 3D worlds that can be integrated into any compatible virtual platform.[103] Additionally, AI can help with the creation of chatbots, avatars and other AI-powered creatures that might be able to help users navigate the metaverse while they look for specific information or socially interact. AI may also be used to produce metaverse data, such as descriptions of virtual worlds or characters.[104]

Another area in which AI is already making a difference in the metaverse is seamless integration.[105] As more people, businesses, and services move into the virtual space, there is a growing need for technology that can facilitate communication and interaction across different platforms and applications. AI-powered tools and systems are helping bridge these gaps, making it easier to interact with the various elements of the metaverse.[106] Likewise, AI is also poised to have a major impact in the metaverse in the realm of language translation. As more people from different parts of the world join virtual spaces, the ability to understand and communicate with one another becomes increasingly important. AI-powered language translation tools are already showing great promise in this area, enabling real-time, fluid text translation and conversations in many languages,[107] which greatly expands the potential audience for the metaverse. Finally, as the metaverse continues to evolve, we will see more ways in which AI enhances experiences in the virtual world – from virtual assistants that help

[102] *See* Cade Metz, *The New Chatbots Could Change the World. Can You Trust Them?,* N.Y.Times (Dec. 10, 2023), https://www.nytimes.com/2022/12/10/technology/ai-chat-bot-chatgpt.html

[103] *Id*.

[104] *Exploring The Role of ChatGPT And The Metaverse*, Finance Monthly, https://www.finance-monthly.com/2023/01/exploring-the-role-of-chatgpt-and-the-metaverse/

[105] AI companies know that this is one of the most important features, and often promise "seamless integration," as well as affordability, and convenience. *See* Georgia Johnson, *Consumer in A Coalmine: Lax Security of Iot Video Devices Puts Corporations Before Users*, 5 Ariz. L.J. Emerging Technologies 1, 5 (2022) (discussing AI-based assistants); ¶ 158-201 Fed Releases Supervision and Regulation Report., Fed. Bank. L. Rep. P 158-201 (discussing FinTech); Iria Giuffrida, Fredric Lederer, Nicolas Vermeys, A *Legal Perspective on the Trials and Tribulations of Ai: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law*, 68 Case W. Res. L. Rev. 747, 757 (2018) (discussing IoT).

[106] *See generally* Yogesh K. Dwivedi et al., *Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy*, Int'l J. of Info. Mgmt 6 (2022) (defining "Metaverse capabilities (MetCap) as the ability of an organization to create a Metaverse environment that allows (goal-directed) users to engage in an immersive experience by enabling the seamless integration of both the physical and virtual world, thereby empowering them to enact value creation activities and transactions that are useful for the business".).

[107] Pete Pachal, *How AI Could Solve the Metaverse's Language Problem,* Coindesk (Jan. 6, 2023), https://www.coindesk.com/business/2023/01/06/how-ai-could-solve-the-metaverses-language-problem/; Annelise Finegan and Elizabeth Haas, *Beyond Language: The Metaverse's New Superpower*, NYU, (Aug. 3, 2022), https://www.sps.nyu.edu/homepage/metaverse/metaverse-blog/digital-twins-an-industrial-win-from-the-metaverse.html (explaining that with more than 7,000 languages spoken, "linguistic barriers have divided humans and prevented coordination across borders," but the "metaverse may soon be able to change that" with seamless communication); *Exploring The Role Of ChatGPT And The Metaverse*, *supra* note 104.

people navigate the metaverse, to new AI-based virtual experiences and more.

C. Decentralized Applications

Decentralized apps (dApps) are a type of software that runs on a decentralized network, as opposed to a centralized server or network.[108] In the context of the metaverse, dApps can provide users with a wide range of services, products and experiences, which are built on blockchain technology, and can be used to create virtual worlds, marketplaces, games, and other decentralized digital experiences that are not controlled by any single entity.[109] In the metaverse, dApps can provide users with an unprecedented level of control over their digital assets and data. Unlike traditional apps, where users' data is stored on centralized servers and controlled by a single company, dApps allow users to retain full control over their data.[110] Some examples of dApps that were developed for use in the metaverse include the following: (i) Decentraland, which thus far recorded low monthly active users (MAU),[111] and is a virtual reality platform built on the Ethereum blockchain, where users can create, experience, and monetize content and applications.[112] (ii) Somnium Space, built on blockchain technology, and allows users to buy, sell, and build on virtual land, create and monetize 3D content, and interact with others in decentralized virtual worlds.[113] (iii) The Sandbox, a blockchain-based virtual world game where players can create, share and monetize their own 3D pixel gaming experiences using NFTs.[114] (iv) Axie Infinity, Binemon, Blankos Block Party, My Crypto Heroes, and Lost Relics, which are all blockchain-based RPG games that have proven somewhat popular and provide cool interactive, art and history and culture-related offerings.[115] But these dApps are still not nearly as popular as the virtual environments and immersive games Roblox, Fortnite, or even Zepeto, which log 202 million, 80 million and 20 million MAUs respectively.[116] DApps can also provide a new level of security and privacy to users in the metaverse, as the blockchain technology – at least theoretically – can provide a higher level of trust and security for users in the metaverse.

[108] *See* Ethereum Explanatory Document, Introduction to Dapps, ETHEREUM, https://ethereum.org/en/developers/docs/dapps.

[109] Chris Brummer, *Disclosure, Dapps and Defi*, 5 Stan. J. Blockchain L. & Pol'y 137, 141 (2022) (noting that dApps enable "new forms of control for consumers insofar as they do not have to hand over personal data.").

[110] For an analysis of this in the context of banking apps, and consumers' inability to manage their banking data, *see* Nizan Geslevich Packin, *Show Me the (Data About the) Money!,* 2020 Utah L. Rev. 1277 (2020).

[111] Ross, *supra* note 89.

[112] Elizabeth Howcroft, *Virtual Real Estate Plot Sells for Record $2.4 Million*, Reuters (Nov. 24, 2021), https://www.reuters.com/markets/currencies/virtual-real-estate-plot-sells-record-24-million-2021-11-23/.

[113] *Elizabeth Howcroft, Metaverse pioneers unimpressed by Facebook rebrand, Reuters (Nov. 1, 2021), https://www.reuters.com/technology/metaverse-pioneers-unimpressed-by-facebook-rebrand-2021-11-01/.*

[114] Elizabeth Howcroft, *Gaming platforms FlickPlay, The Sandbox take steps toward metaverse*, Reuters (April 18, 2022), https://www.reuters.com/technology/gaming-platforms-flickplay-sandbox-take-steps-toward-metaverse-2022-04-18/.

[115] *Blockchain Gaming Market Report 2022: Shift from Traditional Games to Blockchain-Based Games Bolsters Sector*, Yahoo Finance, (Dec. 26, 2022), https://www.yahoo.com/now/blockchain-gaming-market-report-2022-113300103.html.

[116] Ross, *supra* note 89.

II. PRIVACY IN THE METAVERSE: RISKS AND CHALLENGES

To create an immersive 3D space of the metaverse that is highly connected to the physical world, tech developers integrate the various mentioned technologies and others such as rain-computer interfaces (BCI).[117] These technologies collect, store, process, share and monetize vast amounts of data on user-experience on several virtual platforms.[118] Although data is a considered as an important resource for supporting virtual space infrastructures and their primary activities, its immense gathering, use and distribution create novel challenges for protecting privacy in this new digital economy.[119]

The challenges are both practical and legal. At the practical level, the type of data shared—including sensitive biometrical and behavioral data —along with the massive volume needed to power AI-based, immersive digital environments and experiences, make the metaverse a particularly sensitive one in connection with data protection and privacy. Yet, without mass collection and processing of data there could be no metaverse and any immersive experience cannot be sustained. Therefore, in the metaverse, as further described below, data is not only resource, but more importantly, it is the infrastructure itself, which produces a significant legal challenge, particularly for privacy law. Indeed, the primary legal concern is whether current privacy laws, which arguably already demonstrate some insufficiencies in addressing Web2 issues, would be able to protect metaverse users. Especially, when the need to assess privacy violations is in the *prima facie* borderless virtual world of the metaverse. Attempting to better understand these concerns, we start analyzing these issues by grouping privacy risks into three main categories.[120]

A. Personal Information.

The metaverse environment generally allows tech giants, through their virtual platforms, to expand the collection of data by tracking people's personal information,[121] individual locations, body movements, and facial expressions and capturing biometric information.[122] This information enables those collecting it to easily identify users' age, gender, sexual

[117] Stefan Brambilla Hall and Moritz Baier-Lentz, *3 Technologies That Will Shape The Future Of The Metaverse – And The Human Experience*, World Economic Forum (Feb. 7 2022) (noting that the "metaverse will be shaped by technologies used to access it," including VR, AR, and BCI.); Dwivedi *supra* note 106.

[118] *Id*. at 8 ("Metaverse systems can collect far more sensitive information than traditional systems").

[119] Girard Kelly, Jeff Graham, Jill Bronfman, and Steve Garton, *Privacy of Virtual Reality: Our Future in the Metaverse and Beyond* 1–6 (2022), https://www.commonsensemedia.org/sites/default/files/research/report/privacy-of-virtual-reality-our-future-in-the-metaverse-and-beyond.pdf.

[120] Roberto Di Pietro and Stefano Cresci, *Metaverse: Security and Privacy Issues* 4 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (2022), https://arxiv.org/abs/2205.07590.

[121] Maria Lillà Montagnani and Mark Verstraete, *What Makes Data Personal?*, 56 UC Davis Law Review (forthcoming, 2023) (explaining why personal information has to be defined according to the "concept of separability" implying that when the information is indispensable part of the person, it must be considered as personal).

[122] Dwivedi et al., *supra* note 106, at 10.

orientation, race, or disability without their knowledge or consent.[123] Specifically, VR devices,[124] collect biometric data by following users' head and body changes, locating different physiological parameters, such as eye and gaze movements, measuring heart rate, and sensing neural activities related to brain-computer interfaces, like speech activity.[125] Such data is collected and shared with third parties for profiling and marketing customized products.[126] Further, VR devices make it possible to identify and collect data on any bystander within sight of an XR user, even though that bystander chose not to enter the virtual landscape,[127] and through cloud computing products, individuals are exposed to and identified with other users in the virtual world.[128]

Moreover, the metaverse allows participating entities – private and public – to collect data independently, process, and share similar personal information to improve consumer interactions for business purposes.[129] For example, the Meta Quest Pro is its latest VR headset, which tracks eye movements and facial expressions using five inward-facing cameras. Avatars can display real-time expressions, such as smiles, winks, or raised eyebrows.[130] Meta explicitly announced that Meta Quest Pro is based on an opt-in default that allows users to decide whether to share such information with the platform.[131] At the same time, Meta acknowledged that such information is essential for the immersive experience.[132] Consequently, many users will likely share much data to better enjoy the experience.[133]

Although Meta emphasized that raw image data from eye tracking is processed and deleted

[123] Mark McGill, *The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy* (White Paper, 2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf.

[124] Kelly et al., *supra* note 119, at 8–12.

[125] Tom Wheeler, *If the Metaverse Is Left Unregulated, Companies Will Track Your Gaze and Emotions*, Time USA (20 June 2022), https://time.com/6188956/metaverse-is-left-unregulated-companies-will-track-gaze-emotions/ ("The 3-D metaverse utilizes optical equipment to connect the user to algorithms that put them "inside" a pseudo-world.").

[126] Tatum Hunter, *Surveillance will follow us into 'the metaverse,' and our bodies could be its new data source,* The Washington Post (13 January 2022), https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/ (noting that VR "headsets can collect more data about us than traditional screens, which gives companies more opportunities to take and share that data for profiling and advertising.").

[127] McGill, *supra* note 123, at 12.

[128] Dwivedi et al., *supra* note 106 at 12.

[129] Ling Zhu, *The Metaverse: Concepts and Issues for Congress* 19–21 Congressional Research Service (2022), https://sgp.fas.org/crs/misc/R47224.pdf.

[130] Khari Johnson, *Meta's VR Headset Harvests Personal Data Right Off Your Face*, WIRED (October 13, 2022), https://www.wired.com/story/metas-vr-headset-quest-pro-personal-data-face/.

[131] *Meta Quest Pro: Built with Privacy in Mind*, Oculus Blog (October 10, 2022), https://www.oculus.com/blog/meta-quest-pro-privacy/.

[132] *Id*. ("Meta Quest Pro, our next-generation, high-end VR headset, offers opt-in eye tracking and Natural Facial Expressions to let you express yourself in VR far more realistically than ever before.").

[133] On how privacy policies of VR technologies are misleading as to what data is necessary for the user's experience and thus incite misinformed consent, *see* Yeji Kim, *Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent*, 110 Cal. L. Rev. 225, 229 (2022).

once processing is complete,[134] insights collected from these images and abstracted facial expressions could be collected, processed, and stored on Meta servers.[135] Therefore, without data governance adjusted to the metaverse setting, Meta might share eye-tracking data with third-party apps to help them better understand users' interactions and influence them to consume different products.[136] Furthermore, parties could use face and eye movement data to target and exploit people emotionally, and use engage in unfair consumer practices.[137]

B. Behavior

Another type of data analyzed by ML and AI tools powering the metaverse is user behavior. Because avatars represent human users' behavior, choices, and habits, they enable the platform to produce sophisticated analyses of individuals by following their intentions, actions, mental processes, and cognitive experiences. Such an analysis is needed to classify and understand users' consumption practices for marketing purposes.[138] In real-time, retailers can track users' physiological responses, vocal inflections, and facial movements through multiple channels, such as microphones and wearable devices. It provides valuable information to business entities for targeted advertising and profiling, which can be used to personalize customer products and services.[139] Still, collecting information on users' behavior creates a significant concern that such data will be used within the metaverse or outside it to discriminate against users in transactional or personal activities.[140] Also, because many virtual spaces are based on an AI-driven algorithm that analyzes behaviors to generate unique model of users' preferences, the risk of AI biases is intensified.[141]

In addition, data on users' behaviors shared among platforms, business entities, and other parties in the metaverse might be employed for illegal purposes. For example, while the platform will probably share user information with business entities and professional communities for marketing purposes, different stakeholders of such entities might use the data for stalking, sexually-harassing, or cyberbullying – a scenario especially concerning given that virtual have become fertile ground for sexual abuse against minors and females.[142]

Furthermore, the metaverse is ultimately designed to prevent individuals from distinguishing between the virtual and physical worlds.[143] Thus, it might make sense to view virtual assaults

[134] *Id*.
[135] Johnson, *supra* note 105.
[136] *Id*.
[137] *Id*.
[138] McGill, *supra* note 123, at 8–9.
[139] Dwivedi, *supra* note 106, at 27.
[140] *See e.g.,* Nizan Geslevich-Packin & Yafit Lev-Aretz, *On Social Credit and the Right to Be Unnetworked*, 2016 Columbia Bus. L. Rev 339 (2016) (focusing on social behaviors that are used to determine credit scores.)
[141] van Rijmenam, *supra* note 5, at 164–165.
[142] Nina Jane Patel, *Reality or Fiction?: Sexual Harassment in VR, The Proteus Effect and the Phenomenology of Darth Vader — and Other Stories,* Medium (Dec. 21, 2021) (describing how her avatar was verbally and sexually harassed within seconds).
[143] *Id*.

as generating physiological and psychological responses – as if conducted physically.[144] Put differently, in the metaverse, the "potential for the harm to be more insidious and impactful" is substantial as "the realism that accompanies VR experiences readily translates to fear experienced emotionally, psychologically, and physiologically."[145]

C. Interactions.

The metaverse platforms enable numerous and interconnected communications among private individuals, business entities, public organizations, and hybrid bodies across several platforms through various applications simultaneously. These interactions are tracked and processed via VR wearables and devices, which provide more realistic and immersive user-experiences in the metaverse.[146] They are conducted in ways that significantly expand the amount of data collected on users compared to traditional Web2 social platforms, and using AI technology, interactions include verbal, written, visual, nonverbal (body-language), and technical communication between parties. But such AI-powered interactions are never neutral. Indeed, it is now well-documented how biases are programmed into big data algorithms,[147] often resulting in systematically discriminatory and incorrect decision and predictions in all areas of life.[148] For example, an algorithm used by American hospitals to estimate patients' need for additional medical care favored white populations over black ones.[149]

Furthermore, recent studies by researchers from the University College of London have demonstrated that human-AI interactions create a mechanism by which not only biased humans generate biased AI systems, but biased AI systems can change people's perceptual, emotional, and social judgments and distort them more than ever before.[150] Specifically, their experimental studies showed that although human data is marginally biased when conveyed to AI, the latter amplifies any relevant bias. As a result, when humans interact with biased

[144] *Id*. This is especially prevalent in online games, which is one of the primary applications of the metaverse. A recent study indicated that to avoid online harassment, female gamers actively conceal their identities, and lack of social support made them feel anxious, lonely, and sad. These negative emotions are not limited to the virtual landscape and are expressed outside of it too. *See* Lavinia McLean & Mark D. Griffiths, *Female Gamers' Experience of Online Harassment and Social Support in Online Gaming: A Qualitative Study,* 17 International Journal of Mental Health and Addiction 970 (2019).

[145] Sameer Hinduja, *The Metaverse: Opportunities, Risks, and Harms*, Cyberbullying Research Center (11 May 2022), https://cyberbullying.org/metaverse. See Mary Anne Franks, *The Desert of the Unreal: Inequality in Virtual and Augmented Reality*, 51 UC Davis L. Rev. 499, 526–530 (2017).

[146] Lik-Hang Lee et al., *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda* 41 (arXiv preprint, 2021), https://arxiv.org/pdf/2110.05352.pdf.

[147] Nizan Geslevich Packin & Yafit Lev-Aretz, *Learning Algorithms, and Discrimination*, in Research Handbook on the Law of Artificial Intelligence 88 (Woodrow Barfield & Ugo Pagallo eds., 2018).

[148] *Id*. at 96.

[149] Heidi Ledford, *Millions of Black People Affected by Racial Bias in Health-Care Algorithms* 574(7780) Nature 608, 608–610 (2019).

[150] Moshe Glickman and Tali Sharot, *Biased AI Systems Produce Biased Humans* (15 November 2022), https://doi.org/10.31219/osf.io/c4e7r.

AI, they become significantly more prejudiced than they initially were.[151] These results demonstrate that algorithmic bias creates a feedback loop. An AI algorithm trained on limited, biased human data will exacerbate initial human biases due to further interacting with many other humans.[152]

Utilizing AI for linguistic purposes in the metaverse, as referenced above, in 2022, Facebook AI Research (FAIR) released a sizeable multilingual transformer model, No Language Left Behind (NLLB). It aims to enhance the metaverse accessibility to billions of people who cannot communicate in their preferred native languages.[153] Although the model adopts an inclusive approach to interpersonal interactions in the virtual setting, it does not remove the risk of controlling communications among individuals. For instance, the model cannot cover each of the thousands of existing languages effectively and so it will probably direct its efforts to the prevalent ones that match the gatekeepers' business interests. Moreover, the model may normalize these languages in a manner that impairs users' liberty and free speech, and create biased transformations insensitive to different body name systems in various languages, resulting in inherent gender, race, or disability-based discrimination across the metaverse and eventually the physical world.[154]

Although interactions in the metaverse are processed through AI, a recent study showed that their potential value in performance, innovation, and stakeholders' satisfaction is not necessarily superior to interactions made in the Web2 era.[155] However, there is little doubt that the Metaverse involves accumulating countless records of user interactions higher than ever before.[156] The reason is that the concept of data and its relevant functions are understood differently in Web3 compared to the Web2 era.

Specifically, to illustrate this evolution, we distinguish between *data as a resource* and *data as an infrastructure*. In the age of Web2, data is a resource that users consume and upload to

[151] *Id*. at 8.

[152] *Id*. at 8–9 and 20–21. Adopting the opposite position, Orly Lobel argues that by using digital technology, humans have an advantage in detecting discrimination, correcting historical exclusions, subverting stereotypes, and tackling most complex problems. *See* Orly Lobel, The Equality Machine: Harnessing Digital Technology for a Brighter, More Inclusive Future (2022).

[153] Meta, *New AI Model Translates 200 Languages, Making Technology Accessible to More People* (July 6, 2022); https://about.fb.com/news/2022/07/new-meta-ai-model-translates-200-languages-making-technology-more-accessible/.

[154] Phillip Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, 55 Common Market L. Rev. 1143, 1146–1150 (2018); Anna Goldschmidt, *How We Handle Language in the Metaverse May Set the Tone for the Future*, Moeara (March 21, 2022); https://moeara.com/how-we-handle-language-in-the-metaverse-may-set-the-tone-for-the-future/ ("Perhaps more troubling is the fact that we train large-scale AI language models often with data from toxic online interactions. No wonder we see that bias reflected back to us in machine-generated language.")

[155] Thorsten Hennig-Thurau et al., *The Value of Real-time Multisensory Social Interactions in the Virtual-Reality Metaverse: Framework, Empirical Probes, and Research Roadmap* (July 1, 2022), https://ssrn.com/abstract=4090014.

[156] *Id*. at 47 (Metaverse involves "countless records of users activities and user interaction… the accumulated records and traces would cause privacy leakages in the long term.")

pre-developed infrastructures.[157] Therefore, data is an instrument that attracts many users wishing to learn, interact and enjoy.[158] Data as a resource is concentrated in various data centers worldwide, subject to different data localization laws restricting the flow of information across borders to avoid foreign surveillance and security concerns.[159] In contrast, in Web3, data will not merely be created and shared. Instead, it is an essential part of the infrastructure as it is required to create and sustain an immersive experience like the physical world. Consider, for example, the concept of *digital twins (DTs)*.[160] It refers to creating spaces that encompass an equal digital representation of any physical asset, person, process, or operation using data flows across and beyond the metaverse. AI algorithms are employed in processing real-time data to achieve a highly realistic simulation of physical objects and predict their future development and condition.[161]

Furthermore, collecting, processing, and storing data exchanges is not limited to personal interactions. In particular, more and more of such data has been shared in the employment context in recent years.[162] But when such practices are part of employment relationships – as the metaverse enthusiast envision for the case to be – they may undermine employees' reputations as respectful individuals.[163] For instance, companies can use data about users' interactions to gain sensitive information (and make predictions) about sexual preferences or potential physical and mental-illnesses of applicants and evaluate employees' performance.[164] By providing employers with the infrastructure for monitoring employees' interactions the boundaries between employers' prerogatives and employees' personal life are blurred. Consequently, employees are more prone to abuse before, during, and after

[157] Pascal D. König, *Fortress Europe 4.0? An Analysis of EU Data Governance through the Lens of the Resource Regime Concept*, European Policy Analysis 3–5 (2022).
[158] Anita Whiting & David Williams, *Why People Use Social Media: A Uses and Gratifications Approach*, 16 Qualitative Mkt. Rsch. 362 (2013), https://www.emerald.com/insight/content/doi/10.1108/QMR-06-2013-0041/full/html.
[159] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L. J. 677 (2015) (surveying data localization measures and arguing they undermine privacy and security without preventing foreign surveillance of information and increase domestic surveillance risks); H Jacqueline Brehme, *Data Localization: The Unintended Consequences of Privacy Litigation*, 67 Am. U. L. Rev. 927 (2018) (noting that the proliferation of data localization laws increases the government's access to information, cybersecurity threats, and risks to users' privacy).
[160] van Rijmenam, *supra* note 5, at 117–125.
[161] Joshan Abraham et al., *Digital twins: The Foundation of the Enterprise Metaverse* 2 (McKinsey & Company, 2022), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-the-foundation-of-the-enterprise-metaverse.
[162] Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97:2 Indiana L. J, 707, at 743-754 (2022)(noting that the availability of data related to the employment relationship has grown into massive dimensions used to create all sorts of performance and predictive metrics.).
[163] Valerio De Stefano and Mathias Wouters, *AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework* 10–23 (European Parliamentary Research Service, 2022) (describing potential AI-based VR platforms used in labor contexts, such as recruitment, staff assessment, professional performance, encouragement of workers' productivity, and employee retention)
[164] *Id.* at 13–20.

concluding employment relationships.[165] There is little doubt that the increasingly intensifying tracking of employees' interactions requires policymakers to redefine social rights in the digital age.[166] In the context of the metaverse, this requirement will become even more pressing. In sum, privacy risks in the metaverse are intensified by the unprecedented generation, gathering, and exchanging of personal, behavioral, and transactional data. Users will be increasingly incentivized to share more data to enjoy immersive experiences in the metaverse, while the boundaries between private and public spaces will continue to blur.

III. A MULTIDIMENSIONAL CONCEPTUALIZATION OF DATA EXCHANGES IN THE METAVERSE

We suggest perceiving the metaverse as a multidimensional, thus complex, landscape in which various players connect at different levels of time, place, and context. Later, we explore the legal implications of our novel formulation for data governance design. Personal, social, and commercial communications in virtual spaces are carried out in three levels of analysis: *micro* (i.e., the individual), *macro* (i.e., population), and *meso* (i.e., groups).

A. Micro-Based View

Generally speaking, currently, the metaverse enterprise consists of individual projects controlled by a few tech companies, which include Meta, Amazon, Microsoft, and gaming platforms such as Roblox.[167] Although this reality allows for experimentation with cutting-edge technologies in isolation, it does not enable the metaverse ecosystem to move away from the disadvantages of the oligopolistic landscape of Web2 and generate long-term and sustainable values.[168] In fact, despite the decentralization promises of Web3, the metaverse is currently being built primarily by tech giants with abusive histories and tendencies.[169]

[165] To address these concerns, the EU released in April 2021 a proposal for harmonized rules on artificial intelligence. As outlined in the draft legislation, AI systems employed for recruiting and performance evaluation would be considered "high risk" and subject to comprehensive compliance requirements. *See The Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence* (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM/2021/206 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. *See* Section III's discussion accompanied by *infra* notes.

[166] Antonio Aloisi and Valerio De Stefano, Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour 86–147 (2022).

[167] Delloite*, The Metaverse Overview: Vision, Technology, and Tactics* 8 (2022) ("In our still centralized world, there has been no quick creation of decentralized rules to support the Metaverse, and it will not transform easily or quickly from a niche market into a universal consumer group."), https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-metaverse-report-en-220304.pdf.

[168] Patrick Henz, *The Societal Impact of the Metaverse*, 2 Discover Artificial Intelligence 19, 19 (2022) ("As observed with social media platforms, inside the initial competition, various providers had to close their platforms, leading to today's oligopoly… Similar to the attractivity of social media, also the Metaverse requires a high number of active users and service providers (private companies, but also governmental offices), fostering the tendency to an oligopoly.")

[169] This is also reflected in the recent investigations in the United States and Europe exploring Meta's anti-competitive effects and actions. For example, the Federal Trade Commission recently submitted a claim to the

To address this challenge, the pluralistic understanding of decentralized ecosystems (or openness) requires interoperability which refers to the ability of users, through their avatars, to move between virtual spaces – between different metaverses – with their digital assets and personal data.[170] Indeed, the aforementioned tech giants disagree with the use of singular (metaverse) or plural (metaverses) when referring to the metaverse enterprise, with Meta notably insisting that the metaverse is one, not many.[171] In any event, a metaverse that facilitates interoperability allows disparate, heterogeneous platforms and networks to communicate transparently and exchange objects, behaviors, and avatars easily.[172] Like our bodies moving between physical locations without interrupting their experience, interoperability allows users to transition from one virtual environment to another without losing their digital assets or adjusting login credentials.[173] As a result, any data exchange, data collection and processing is not limited to one space and time. Instead, it will be made on and across several platforms by numerous players interacting simultaneously. Based on the interconnectivity pattern of any data exchange in the metaverse, we perceive platforms and data exchange within them as an expression of complex system theory.[174]

US District Court for the Northern District of California against Meta Platforms Inc. The claim aims to prevent the acquisition of Within because it would "tend to create a monopoly" in the virtual reality (VR) fitness apps market. *See FTC Seeks to Block Virtual Reality Giant Meta's Acquisition of Popular App Creator Within* (July 27, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/07/ftc-seeks-block-virtual-reality-giant-metas-acquisition-popular-app-creator-within. Also, the European Parliament instructed the Commission to ensure that companies in the Metaverse comply with the relevant digital legislation and competition rules. See, The European Parliament, Motion for a European Parliament Resolution on Competition Policy – Annual Report 2021 (2021/2185(INI)), https://www.europarl.europa.eu/doceo/document/A-9-2022-0064_EN.html.

[170] Different laws and authors considered the idea of interoperability. The European Directive on the legal protection of computer programs (Directive 2009/24/EC) defines interoperability between computer systems as "the ability to exchange information and mutually to use the information which has been exchanged."; Marc Bourreau, Jan Krämer, and Miriam Buiten, *Interoperability in Digital Markets* 13 (Centre on Regulation in Europe, 2022) ("[d]ifferent products or services are interoperable if they can 'work together,' meaning that some common functionalities can be used indifferently across them, typically via appropriate information exchange").

[171] Meta*, Economic Opportunities in the Metaverse: A Policy Approach* 6 (December 2, 2022) ("As regulators consider whether new regulations are needed, we would encourage them to evaluate how to make use of existing concepts and exemptions in light of the specific nature of a given blockchain use case. Moreover, they should focus on principles rather than imposing rules too soon."), https://about.fb.com/wp-content/uploads/2022/12/Economic-Opportunities-in-the-Metaverse_-A-Policy-Approach.pdf. See also, Emily Birnbaum, *Meta Urges Washington to Take Hands-Off Approach to Regulating the Metaverse*, Bloomberg (December 2, 2022), https://www.bloomberg.com/news/articles/2022-12-02/meta-urges-washington-to-take-hands-off-approach-to-regulating-the-metaverse?utm_campaign=socialflow-organic&utm_medium=social&utm_source=twitter&utm_content=crypto&leadSource=uverify%20wall.

[172] Levan Nanobashvili, *If the Metaverse is Built, will Copyright Challenges Come?,* 21 UIC Rev. Intell. Prop. L. 215, 236 (2022) ("If interoperability is achieved, it could be possible to travel among different Metaverse platforms without changing one's identity or avatar.").

[173] Zhu, *supra* note 129, at 7 ("Interoperability would allow users to move between virtual spaces and access different platforms and services using the same devices and digital assets (e.g., digital identity, currency, and objects.").

[174] Cindy Gordon, *Accelerating Growth Using AI - A Look At Complexity And The Metaverse*, Forbes (February 1, 2022), https://www.forbes.com/sites/cindygordon/2022/02/01/accelerating-growth-using-aia-look-at-complexity-and-the-metaverse--blog-series-15/?sh=11f5a0c66261.

Complex systems theory is based on three fields of study: General System Theory, Cybernetics, and AI.[175] A complex system consists of several elements that interact with each other as nodes in a network. Interactions can be expressed as physical, chemical, social, or symbolic connections.[176] These systems are defined by interactions not being independent but evolving together. Therefore, complex systems are context-dependent because dynamic processes occurring on one layer of a network can influence interactions on other layers (regardless of whether the networks are in single or multiple-dimensional spaces), as shown in figure 2.

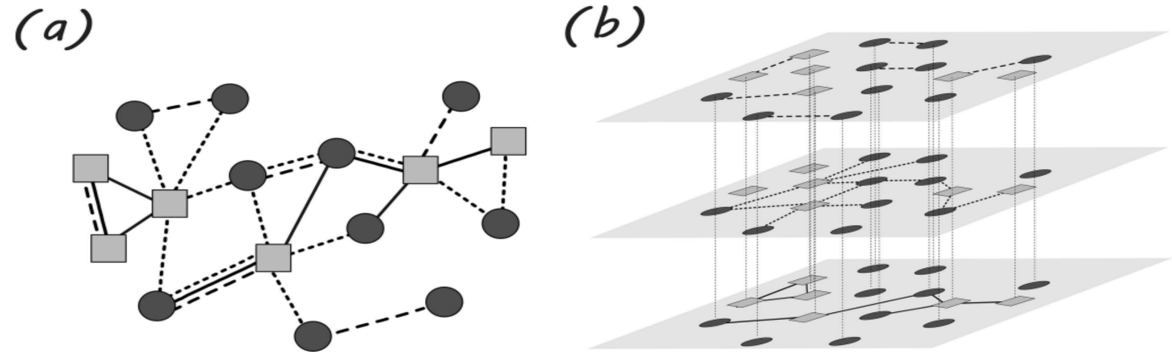

Figure 1: Illustration of complex systems.[177]

The complexity idea perceives states, institutions, and organizations as dynamic structures whose components communally communicate through "collective behavior, sophisticated information processing, and adaptation via learning or evaluation."[178] As part of these communications, any actor's interaction influences and, at the same time, is influenced, directly or indirectly, by interactions made by other components in the system.[179] Moreover, when a system is complex, we cannot set a strong borderline between the system, its members, and the environment. This is because the environment "co-constitutes the identity" of the system and gives rise to its non-linearity dynamic interactions.[180] Through interacting, observing, communicating, and adjusting, patterns of interaction are disseminated, leading to an overall program.[181] This program reflects a nonlinearity quality in which the sum of the system's parts is greater than the collection of the parts as if they were in isolation. Generally,

[175] Yasmin Merali & Peter Allen, *Complexity and Systems Thinking*, in The SAGE Handbook of Complexity and Management 31, 32–33 (Peter Allen, Steve Maguire, Bill McKelvey eds., 2011); David Byrne and Gillian Callaghan, *Complexity Theory and the Social* Sciences: The State-of-the-Art 47 (2022).

[176] Stefan Thurner, Rudolf Hanel, and Peter Klimek, Introduction to the Theory of Complex Systems 21–23 (2018).

[177] *Id*. at 21.

[178] Rika Preiser and Minca Woermann, *Complexity, Philosophy, and Ethics*, in Global Challenges, Governance, and Complexity 38, 39 (Victor Galaz ed., 2019).

[179] *Id*. at 44.

[180] *Id*.

[181] Volker Schneider, *Governance and Complexity*, in The Oxford Handbook of Governance 129, 135 (David Levi-Faur ed., 2012).

linear relationships can take one of the following forms:[182]

$$(1) \quad f(x+y) = f(x) + f(y)$$

$$(2) \quad f(cx) = c\, f(x), \text{ where c is any constant.}$$

A nonlinear function is any function that does not follow these equations. For example, the Web is a complex system that contains a network of the Internet structural function and a network of hypertext links between web pages. The connections across these networks cannot be considered entirely linear.[183]

The metaverse is a prominent expression of a complex system with simultaneous intertwined data interactions among players at several virtual platforms. Data exchanges among various players on different platforms are unlimited and interconnected. Like how the internet is perceived as a "global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols,"[184] the metaverse is a global system of virtual environments that uses standardized communication protocols to facilitate the exchange of information between networks.[185] Moreover, because we perceive data as the building blocks of the metaverse infrastructures, removing (or significantly constraining) one element from the system undermines its ability to provide immersive experiences to users.[186]

Under the *public view* – the second scenario for the development and popularity of the metaverse – the metaverse will be developed into a decentralized system that no single entity controls, data interactions are made across several virtual platforms by numerous players concurrently. As Matthew Ball puts it, metaverse users experience a "*continuity* of data, such as identity, history, entitlements, objects, communications, and payments."[187] To illustrate this observation, consider the Nike-created metaverse space utilizing the Roblox platform to allow its fans to interact with their favorite brands, meet new people and participate in promotions. As part of such collaboration, we can assume that the platform shares valuable user information, including user identity, behavior, and social and commercial interactions, with Nike to enhance the marketing of sports products and promote the brand.[188] Based on the idea of interoperability and assuming the public understanding of the metaverse is materialized, data exchanges among players will *not* be limited solely to a single place or time within one platform. Because many businesses and other entities, such as Nike, will

[182] James Ladyman and Karoline Wiesner, What Is a Complex System? 13–14 (2020).
[183] *Id*. at 54–57.
[184] The Oxford Dictionary of Phrase and Fable 354 (Elizabeth Knowles ed., 2006).
[185] Dwivedi et al., *supra* note 106, at 23.
[186] John Miller & Scott Pag, Complex Adaptive Systems: An Introduction to Computational Models of Social Life 9 (2007).
[187] Matthew Ball, *Framework for the Metaverse*, MatthewBall.VC (29 June 2021), https://www.matthewball.vc/the-metaverse-primer.
[188] Bernard Marr, *The Amazing Ways Nike Is Using the Metaverse, Web3, and NFTs*, Forbes (1 June 2022), https://www.forbes.com/sites/bernardmarr/2022/06/01/the-amazing-ways-nike-is-using-the-metaverse-web3-and-nfts/?sh=153253a656e9.

operate on multiple platforms, any user data gained within one platform will likely be used to leverage the activities of those entities on other platforms. Thus, if a user employs her avatar to interact with other parties on a certain platform, data exchanges related to user interactions could be made within other platforms and among different players, even though that user is currently *not* present on those platforms. Put differently, because the same players will be present on multiple platforms altogether, the collection, processing, and sharing of user data between them will take place even if the user does not explicitly interact with them on each platform. The traditional civil liability assumes a linear and static relationship between the parties which allows identifying a clear cause and effect manifested in single dimension of time and place. In contrast, complex understanding of civil liability in the metaverse is based on a non-linear and dynamic relationship between the wrongdoer and the injured party across several platforms simultaneously which removes our ability to observe a clear causal relationship.

Consequently, data exchanges in the metaverse create privacy relationships among players that are *not* merely interrelated, but instead, are dispersed, unlimited and interconnected. The following figure introduces the *micro-level description* of the metaverse's *interdependent* data exchanges.

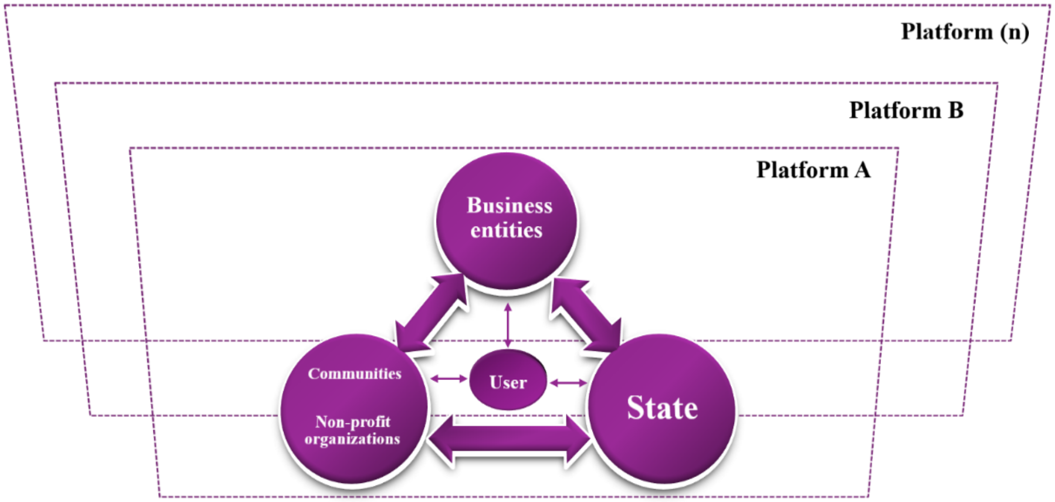

Figure 2: The micro level of the metaverse.

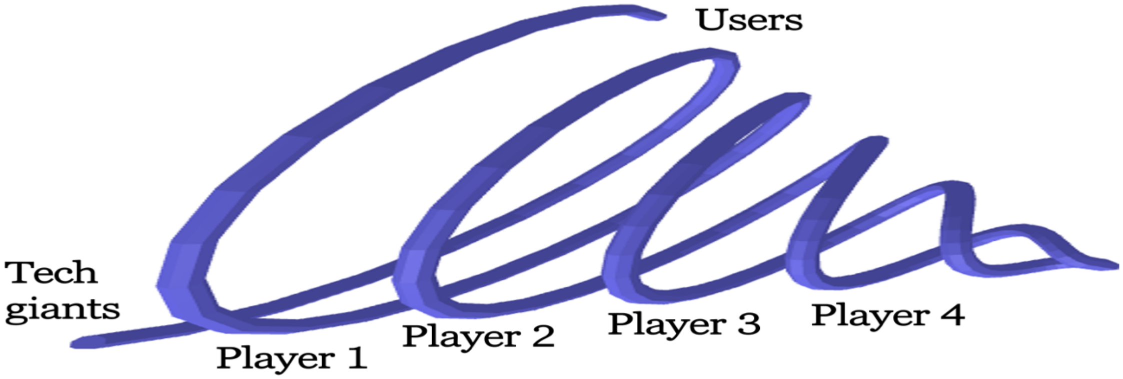

Figure 3: The complex understanding of civil liability in the metaverse

B. Macro-Based View

A macro-based view of the metaverse requires us to zoom out from the individual and complex interpersonal relationships and observe the connections between the tech giants developing the metaverse and populations of various parties interacting on the virtual platforms. These populations can be distinguished and grouped based on identifiable, sensitive characteristics: age, gender, race, sexual preferences, and socio-economic background. The macro-based view forces us to rethink individualistic data protection models and focus on the collective nature of privacy risks in spaces like the metaverse.

As discussed above, to enable faster computing and a smoother user interface and provide instant and seamless translation of massive amounts of text, images, and videos, the metaverse integrates machine learning technologies and AI for analyzing immense quantities of data.[189] AI enables the extraction of biometrical information to improve virtual infrastructures' performance.[190] Moreover, it extracts personal data to create a model that describes populations' behaviors and identities in several virtual spaces at different times.

As Salomé Viljoen recently argued, the relationships among data subjects, data producers, and third parties in various platforms could be expressed along two axes.[191] The vertical axis stipulates data exchanges between an individual collector and an individual data subject governed by traditional consumer and privacy laws. This view focuses on analyzing the legality of data exchanges between two respective parties by relying on liberty and autonomy values. In particular, the privacy laws regime views data as an "individual medium" whose transmission to others can cause individual harm.

In contrast, the horizontal axis describes how data processing is made, not necessarily by referring to individual data collectors and subjects. Instead, data collection is made in relation

[189] *Supra* note 97–100 and the accompanying text.
[190] Thien Huynh-The et al., *Artificial Intelligence for the Metaverse: A Survey* 4 (2022) https://arxiv.org/pdf/2202.10336.pdf.
[191] Salome Viljoen, *A Relational Theory of Data Governance*, 131 Yale L. J. 573 (2021).

"to one another and to others that share relevant population features with the data subject."[192] Under this view, any data collection might create harmful consequences for specific individuals and numerous individuals who share similar identities, backgrounds, and qualities to those data subjects. Thus, data exchanges at the macro level consider the privacy challenge and the necessity of data governance to address it as a "sociality problem."[193] Accordingly, privacy laws must depart from the individualistic account and consider social costs, and benefits involved in the processing and sharing of data on populations and predefined socio-economic groups.[194]

Therefore, privacy law must consider the vulnerabilities of different populations that experience different harms as a result of power dominance of tech giants.[195] To illustrate this argument, consider the difference between *structural (or systematic)* and *circumstantial vulnerabilities*.[196] *Structural vulnerability* refers to the idea that certain groups, such as minors, do not possess the required awareness, cognitive independence, and decisional capabilities.[197] These ontological features of children define them as such and make them prone to certain risks without the ability to protect themselves.[198] The United Nations Convention on the Rights of the Child (UNCRC) recognizes the particular vulnerability of children, emphasizing that children need special care and protection due to their physical and mental immaturity.[199] The UNCR obligates governments to take protective and preventative measures to combat child maltreatment and to provide parents with facilities, services, and institutions to assist them in meeting their responsibilities.[200] As a result of children's weaknesses, they cannot understand the risks and challenges involved in data-driven architecture and are more predisposed to manipulation and harm in the online setting.[201]

Circumstantial vulnerability assumes that the condition of weakness may vary from one person to another by taking into account different considerations, such as time, place, life background, and even moral luck.[202] Such groups include people with disabilities and asylum

[192] *Id*. at 607.
[193] *Id*. at 603.
[194] *Id*. at 608.
[195] Gianclaudio Malgieri and Jedrzej Niklas, *Vulnerable Data Subjects*, 37 Computer Law & Security Review 10415, *2 (2020); Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DePaul L. Rev. 591, 593 (2017) ("The first is that no one is entirely invulnerable at all times and in all contexts. We are all vulnerable in degrees and according to circumstance.").
[196] Malgieri and Niklas, *supra* note 195, at 3.
[197] Malgieri and Niklas, *supra* note 195, at 5.
[198] Gottfried Schweiger, *Ethics, Poverty and Children's Vulnerability*, 13(3) Eth. & Soc. Welfare 288, 289 (2019).
[199] See *generally*, OECD, Changing the Odds for Vulnerable Children: Building Opportunities and Resilience (2019).
[200] *Id*. at 17.
[201] Malgieri and Niklas, *supra* note 195, at 5.
[202] Florencia Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, International J. Feminist Approaches to Bioethics 121, 129 (2009) (Instead of "thinking that someone is vulnerable," we should consider "a particular situation that makes or renders someone vulnerable.")

seekers.[203] Several studies pointed out the limited capability of deprived groups to allocate the economic and educational resources needed for acquiring the "tools and strategies that would help them protect their personal information."[204] Because these populations cannot adopt (or rely on) effective privacy-protective measures, they are more likely to suffer from noteworthy harms resulting from violations of their rights, such as discrimination in employment, limited access to higher education, and a higher chance of suffering from police enforcement actions. By applying these concepts in the metaverse, privacy laws should also take into account the unique power imbalances and sensitivities. Many jurisdictions address these vulnerabilities by considering the special risks associated with AI-systems to different populations.

The EU legislator, for instance, has since 2018 initiated efforts to regulate AI and set global standards[205] based on a risk-based approach.[206] The AI Act proposal, presented by the Commission in 2021 and soon to be adopted,[207] follows an EU legislative tradition of regulating risk and uncertainty under the so-called 'precautionary principle.'[208] Taking a risk-based approach to regulating the risks associated with AI systems, the AI Act identifies four levels or risk: (*i*) unacceptable risk posed by "particularly harmful" AI practices which the Act prohibits; (*ii*) high risk AI systems which the Act permits under well-defined conditions; (*iii*) low and (*iv*) minimal risk AI systems.[209] The Act describes four categories of prohibited practices, listed under Title II, which are considered unacceptable as contravening Union values, especially when violating fundamental rights such as the right to privacy. Indeed, the legislators' description includes practices that we identified as problematic when discussing privacy risks in the metaverse: "(a)the […] use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's

[203] Malgieri and Niklas, *supra* note 195, at 3.

[204] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash. U. L. Rev. 53, 118 (2017).

[205] On the 2018 European Strategy on AI *see* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe COM/2018/237 final, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.

And more generally on the European Approach to Artificial Intelligence see https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[206] Julia Black, *Risk-based Regulation: Choices, Practices and Lessons Being Learnt* (Risk and Regulatory Policy: Improving the Governance of Risk, OECD Publishing 2010).

[207] Commission, *Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence* (2021), at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

[208] The principle emerged in German domestic law in the early 1970s mainly to address environmental risks. It evolved to apply to cases beyond environmental law and was adopted in various jurisdictions either as soft law principle and or a hard rule applied to cases that involve degrees of risk and uncertainty. *See* Cass Sunstein, Laws of fear: beyond the precautionary principle (CUP 2005); René von Schomberg, *The Precautionary Principle: Its Use Within Hard and Soft Law,* 3(2) European J. of Risk Reg. 147 (2012); Stephen M. Gardiner, *A Core Precautionary Principle*, 14(1) J. of Political Philosophy 33, 33–60 (2008).

[209] Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 [hereinafter AI Act]

behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm" and "(b)the […] use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm".[210] In these two categories, the prohibition applies across the board, to both public and private actors. Thus, private entities such as tech platforms must also comply. The third category prohibits certain practices only when they come from public authorities or on their behalf.[211] Most relevant for our purposes, the fourth category focuses on the "the use of 'real-time' remote biometric identification systems in publicly accessible spaces" targeting only uses for the purpose of law enforcement.[212] This prohibition can be both directly and indirectly applicable to practices in the metaverse, particularly when private actors collaborate with public authorities for law enforcement purposes.[213]

[210] Article 5 AI Act.

[211] Article 5.1(c) AI Act.

[212] Article 5.1(d) of the AI Act:
1. The following artificial intelligence practices shall be prohibited:
[…]
(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:
(i)the targeted search for specific potential victims of crime, including missing children;
(ii)the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
(iii)the detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.
2.The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:
(a)the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
(b)the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

[213] Currently, in the U.S. several states – Illinois, Texas, and Washington – have enacted biometric laws, but only the Illinois Biometric Information Privacy Act (BIPA) provides individuals with a private right of action. *See The evolution of biometric data privacy laws,* Bloomberg (Jan. 25, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/#:~:text=The%20Illinois%20Biometric%20Information%20Privacy%20Act%20(BIPA),-In%202008%2C%20Illinois&text=The%20law%20requires%20entities%20that,damages%20when%20they%20do%20not. The A decade after its enactment, a few cases have made it easier to file BIPA suits. First, in 2019, the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.* determined that a plaintiff can be considered an "aggrieved person" under the law and "be entitled to liquidated damages and injunctive relief" without alleging an actual injury. Afterwards, in 2020, the U.S. Court of Appeals for the Seventh Circuit *in Bryant v. Compass Group USA, Inc.* confirmed that such a person has suffered an injury-in-fact sufficient to support standing under BIPA Section 15(b). Likewise, in 2020, a class action lawsuit *Patel v. Facebook, Inc.* reached a conclusion when Facebook agreed to a $650 million settlement in order to resolve claims it collected user biometric data without consent. Finally, in 2022, a jury verdict in a BIPA class action lawsuit was handed down *in Rogers v. BNSF Railway Company*. *Id.*

Under specific accumulative conditions, AI systems that constitute a safety component of a product are classified as high-risk.[214] In addition to those, Annex III of the Act lists eight more practices or systems that are also considered high-risk.[215] There are: 1. 'real-time' and 'post' remote biometric identification of natural persons, 2. AI systems used for the management and operation of critical infrastructure, namely as road traffic and the supply of water, gas, heating and electricity, 3. systems used in educational and vocational training institutions including for the purposes of determining access to the latter, 4. systems used for recruitment, decision-making relating to evaluation and promotion, as well as for monitoring in work contexts, 5. systems determining access and enjoyment of essential private and public services and benefits (including creditworthiness, priority in dispatching of emergency first response services etc.), 6. systems indented for law enforcement purposes and 7. for migration, asylum and border control management and, lastly, 8. AI systems intended to assist authorities in the administration of justice and in democratic processes.[216]

To mitigate the identified as high-risk practices, the Act introduces a number of compliance requirements which include the a risk management system,[217] and "appropriate data governance and management practices" for the training, validation, and testing of data sets used.[218] Other safeguards include the requirement of technical documentation,[219] record-keeping,[220] and transparency obligations.[221] When designed and throughout their lifecycle, high-risk AI systems must be developed to achieve "an appropriate level of accuracy, robustness and cybersecurity" with appropriateness being measured in accordance to the system's indented purpose.[222] Last but not least, for high-risk AI systems the Act requires human oversight through "appropriate human-machine interface tools."[223] The Act imposes only transparency obligations to "certain", or else low-risk AI systems under Article 52.[224] The provision requires that: 1. natural persons must always be informed that they are interacting with an AI system, 2. natural persons exposed to emotional recognition or biometric categorization systems shall also be informed, unless the biometric categorization is permitted by law for the purposes of detection, prevention, and investigation of criminal offences, and 3. deep fake content is disclosed. All other AI systems not captured by the above three umbrella categories of risk, namely unacceptable, high, and low risk, are not regulated as entailing minimal risk.

As acknowledged in the Act's explanatory memorandum, risk-based regulatory approaches

[214] Article 6 AI Act.
[215] Annex III of the AI Act.
[216] *Id*.
[217] Article 6 AI Act.
[218] Article 9 AI Act.
[219] Article 11 AI Act.
[220] Article 12 AI Act.
[221] Article 13 AI Act.
[222] Article 15 AI Act.
[223] Article 14 AI Act.
[224] Article 52 AI Act.

must define the risk regulated with accuracy and be proportionate, meaning that legal intervention must be tailored to concrete cases "where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future."[225] However, when we look at the Act's large category of high-risk AI systems as described above it is, arguably, not an ideal example of accuracy or proportionality. The practices and systems as listed in the Act's Annex III are very broadly defined, even if they are a closed number, and in fact encompass various degrees of risk which the Act places under a blanket high-risk umbrella. Even if the effort to create risk-mitigating rules that are flexible enough to apply to various technologies and that accommodate technological evolution is not an easy task, the risk of non-well defined risk categories is not negligible. Such rules can be very hard to apply in practice both by parties who try to comply, especially by small players such as Small and Medium-Sized-Entities (SMEs), and by courts who will be asked to assess compliance. Thus, such rules may distort market incentives and create inefficiencies.[226] This category is also likely the most relevant to practices and systems employed by metaverse entities. Thus, once these rules are adopted and become law across the EU they will affect the development of metaverse services in the continent.

Following these early attempts to regulate AI coming from Europe, more jurisdictions including Brazil Canada and the US are now considering similar laws. The latest effort coming from the US is the presidential Blueprint for an AI Bill of Rights.[227] The Blueprint is a noticeable effort particularly because it promises data privacy protection at the federal level.[228] The bill introduces a right to "be protected from abusive data practices via built-in protections" and agency over the use of ones' data.[229] While being fundamentally consent-centric, data privacy provision embraces privacy by design and by default.[230] The provision focuses particularly on the design of consent mechanisms. It can also be read as adopting, at least indirectly, a risk-based or rather tiered approach distinguishing cases of "sensitive domains" which include health, work, education, criminal justice, and finance, and for data

[225] AI Act, Exploratory Memorandum.

[226] Roee Sarel, *Restraining ChatGPT* (February 11, 2023), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4354486

[227] White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/
Similar efforts in Canada are linked to Bill C-27, the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. Brazil was as fast as the EU in considering the introduction of rules specifically on AI after the launch of the Brazilian Strategy for Artificial Intelligence and with the introduction of the National Draft Bill on Artificial Intelligence: Marco Legal da Inteligência Artificial, PL 21/2020. See Luca Belli, Yasmin Curzi and Gaspar Walter, *AI Regulation in Brazil: Advancements, Flows, and Need to Learn from the Data Protection Experience*, 48 Computer Law & Security Review (2023), https://www.sciencedirect.com/science/article/abs/pii/S0267364922001108

[228] White House, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/.

[229] *Id*.

[230] *Id*.

pertaining to youth as well as surveillance technologies.[231] For these sensitive domains the provision suggests necessity assessments, akin to a data minimization principle, and "heightened oversight" as well as impact assessments.

However, even if the AI Bill adopts a "rights" language, this Blueprint is defined as a set of five "principles" with data privacy being one of those.[232] The first principle calls for protection against unsafe or ineffective AI systems and asks for the involvement of experts in identifying risks prior to deployment.[233] The second principle calls for protection against algorithmic discrimination, the third is the data privacy principle, as discussed above, and fourth is a transparency principle requiring notice and explanation of the AI system's outcomes and impact on individuals.[234] Lastly, the fifth principle calls for opt-out options and remedies.[235] While the principle-based approach is a necessary start, as it stands the Blueprint is rather light-touch and lacks the normativity that one would wish, especially when compared with the EU's AI Act.

The regulation of AI risks can complement or even overlap with data protection laws, as is the case with the EU's GDPR, also a risk-based regulation that precedes the AI Act.[236] In fact, AI-specific regulation can sometimes overlap or even contradict pre-existing data protection regulation. For instance, the relationship between the AI Act and the GDPR might be problematic in two respects: first, with regard to the GDPR's right to erasure – the notorious right to be forgotten – and second, with regard to the Regulation's data minimization principle. The application of both these data protection rules, which now form guaranteed rights for EU citizens, will be challenging in the metaverse. [237]

Critical voices of the EU's legislative efforts have pointed to the risks of overregulation and of implementing contradicting regulatory regimes (along with the AI Act, the EU is also introducing the AI Liability Directive[238] while revising its Product Liability Directive[239]). While the said efforts present significant progress in setting regional and perhaps also global standards for regulating AI, they present a mostly linear understanding of data exchanges.

[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] In both the GDPR and the AI Act risk is employed as a proxy. *See* Raphaël Gellert, *The Role of the Risk-based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?* 3(2) Journal of Ethics and Legal Technologies 15 (2021).
[237] Vagelis Papakonstantinou & Paul De Hert, *EU Lawmaking in the Artificial Intelligent Age: Act-ification, GDPR Mimesis, and Regulatory Brutality,* European Law Blog (July 8, 2021), https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/.
[238] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.
[239] Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, COM (2022) 495 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495

For example, Roee Sarel recently suggested that AI policies must better integrate law and economics concepts specifically when it comes to proposing liability schemes.[240] Critiquing the EU's AI Act and AI Liability Directive proposal, Sarel argues that these new laws may lead to situations of over- and under-compliance in the market to fit de-facto forming dichotomy between high-risk and non-high-risk AI systems.[241] Despite their ability to protect the privacy interests of different populations on a macro level, these laws do not offer the nuance that AI systems require at a micro level. By focusing on strict liability and negligence as the only liability regimes available to address data exchanges on AI systems, these legislations ignore the non-linear patterns of data relationships that are not subject to traditional principles of causality. To find a more efficient solution, Part IV below explores how setting mandatory privacy obligations on metaverse entities can better mitigate risks associated with AI technologies a priori rather than post-harm.

C. Meso-Based View

Data exchanges on various virtual platforms result from engaging in social, commercial, and professional activities, such as gaming, transactions, and employment interactions. metaverse's potential to provide a unique user-experience is related to the ability of business entities and organizations to use virtual environments and enrich interactions with users, customers, and employees. To that end, each entity or organization operating in the metaverse must process and share relevant information about the user's identity, behavior, and interactions for establishing (profitable) contractual relationships with different stakeholders, such as employees, shareholders, consumers, and suppliers.[242] However, any potential privacy violation in this context is similar to one that would have been made outside such a setting and is merely *incidental* to operating on sophisticated infrastructures of the virtual spaces.

In other words, privacy breaches at this level of analysis are not necessarily associated with interacting in a complicated virtual environment. Instead, they are related to the ability of business entities and organizations to generate revenues by using sensitive information on user-experience. Therefore, the meso-level analysis focuses on the linear and static data relationships created between the business entities and their stakeholders independently as part of their organizational structure by excluding the ability of tech giants to control these engagements by manipulating the infrastructures themselves.

Thus far, we conclude that unlike the micro and macro levels, at the meso-level traditional legal tools to analyze and address privacy concerns are sufficient. Nevertheless, existing

[240] Roee Sarel, Restraining ChatGPT (February 11, 2023), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4354486.

[241] *Id*. at 54–63.

[242] Marco Marabelli and Sue Newell, *Everything You Always Wanted to Know about the Metaverse (But Were Afraid to Ask,* Academy of Management Proceedings 15–20 (2022), https://www.researchgate.net/publication/359472101_EVERYTHING_YOU_ALWAYS_WANTED_TO_KNOW_ABOUT_THE_METAVERSE_BUT_WERE_AFRAID_TO_ASK.

doctrine and theories of privacy, which correspond to legal frameworks applied in Web1 and Web2, are not sufficient for our multidimensional conceptualization of Web3 and the metaverse which includes all three levels of analysis, micro, macro, and meso.

D. The Multidimensional Conceptualization and Theories of Privacy

The metaverse must be perceived as having different operations levels that call for special regulatory measures for each. When designing regulatory responses, we need to consider related privacy theories that correspond to the challenges presented in each level of analysis.[243] The *micro-level analysis* perceives the metaverse as a reflection of a complex adaptive system in which the data exchanges among players in the virtual spaces are interconnected. Specifically, any data relationships between given players are inherently context-dependent because they are influenced by and influence other data exchanges on the platform and are all considered dependent on each other.[244] Consequently, data governance design is not limited to the legal relationship between two parties alone. It must consider other parties' interests that might also be affected by any data transmission.[245] The micro-level understanding can be associated with the contextual integrity (CI) framework of Helen Nissenbaum, who defined privacy as the appropriate flow of information based on whether the flow conforms with contextual informational norms.[246] To establish conformance, a privacy norm requires stipulating five key parameters: information type (about what), subject (about whom), sender (by whom), recipient (to whom), and transmission principle (flow under what conditions).[247] Although these parameters are essential to determine whether certain privacy norms have been violated, their potential application for regulating the micro level of the metaverse is limited. Nissenbaum's framework recognizes that people interact within a wide variety of contexts which requires exploring and fulfilling people's expectations regarding data governance.[248] However, data exchanges in the metaverse are made across several platforms simultaneously and among multiple private and public players. Because data exchanges are not only impacted by each other but also interconnected and conditional on one another, it is challenging to point at specific expectations as to who would get exposed to the data, or what it would be used for. Moreover, it is even difficult to isolate a specific location where a data breach concerning the collection, storage, and processing of personal information has been made. As a result, identifying ordinary data violations and understanding whether certain privacy norms might have been violated could be potentially challenging.

[243] For a general overview of privacy theories, *see, e.g.,* Pamela J. Wisniewski and Xinru Page, *Privacy Theories and Frameworks*, in Modern Socio-Technical Perspectives on Privacy 15 (Bart P. Knijnenburg et al. eds., 2022).

[244] *Supra* note Section III, part A and the accompanying text.

[245] *Supra* note Section III, part A, B and C and the accompanying text.

[246] *See*, *generally,* Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (2010).

[247] *Id*. at 129–157 and 186–230.

[248] *Id*. at 231.

The *macro-level analysis* of the virtual spaces focuses on the interests of populations interacting on virtual platforms vis-à-vis the tech giants who constantly develop infrastructures employing user data. Because personal data is part of the metaverse structure, users cannot be considered merely one out of many relevant stakeholders who are contractually connected to the tech giants. Instead, because user data is critical and essential for the metaverse enterprise's success, data exchanges are not a reflection of arm's length interactions between parties who act independently and in their self-interest.[249] The infrastructure's overall practical function (and potential profitability) is conditional upon data transmission assets that several vulnerable populations provide to enable the immersive experience in the virtual spaces. Because tech giants have a direct commercial interest in obtaining sensitive data required for developing their platforms and increasing consumer and business demand for their infrastructures, they must be subject to special fiduciary obligations that deviate from arm's length dealings.[250]

The macro-level understanding is highly associated with considering privacy law as directed toward protecting private information in the context of trust.[251] Virtual platforms must act trustworthy because different populations entrust their information to them.[252] Platforms could be considered "fiduciaries of our data: we are vulnerable to them, we depend on them, and they hold themselves out as experts and trustworthy."[253] As a result, they should be subject to duties of care, confidentiality, and loyalty.[254] For example, duties of care would require them to employ reasonable measures to secure our data.[255] To maintain confidentiality, they must collect only the data necessary to allow the immersive and persistent experience without damaging users for the purpose of generating profits.[256]

The *meso-level analysis* focuses on the privacy relationships that are not the result of interacting in sophisticated infrastructures, such as virtual spaces. Instead, they are related to effectively rendering products and services like in the physical world. This view recommends understating potential data breaches per the traditional concept of control and access.[257] Based on this approach, privacy refers to a person's exclusive right to access her personal

[249] Daniel Markovits*, Promise as an Arm's-length Relation,* in Promises and Agreements: Philosophical Essays 295, 295 (Hanoch Sheinman ed., 2011) ("promises characteristically arise among strangers and, indeed, that the immanent structure of the promise relation is in itself distancing, which is to say opposed to intimacy.")

[250] Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 Harvard Law Review Forum 11, 25–26 (2020).

[251] See *generally*, Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age (2018); Jack M. Balkin, *Information Fiduciaries, and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1205 (2016). But see Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 498 (2019).

[252] Neil M. Richards and Woodrow Hartzog, *Privacy's Trust Gap* 126 Yale Law Journal 1180, 1185 (2017).

[253] Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox',* 31 Current Opinion in Psychology 105, 108 (2020)

[254] *Id*.

[255] *Id*.

[256] *Id*.

[257] Ruth Gavison*, Privacy and the Limits of Law*, 89 Yale L. J. 421, 423 (1980).

information.[258] For example, Ruth Gavison argued that privacy is best understood as a concern for limited accessibility as part of promoting "liberty, autonomy, selfhood, human relations, and furthering the existence of a free society."[259] Basically, it deals with what others know about us, how physically accessible they are to us, and how much attention they pay to us.[260] However, the propertarian explanation for the meso-level analysis is justified only when it disconnects the collecting, processing, sharing, and using of personal data from the platform's infrastructures. Since tech giants provide businesses and organizations with the setting to conduct social and commercial activities, virtual structures are already predefined and developed. This results in user data not being used for improving the metaverse's infrastructure but rather for optimizing and utilizing the rendering of products and services. Therefore, regardless of whether data violations occur in the physical or virtual worlds, the law should treat them similarly.

IV. A MARKET-BASED SOLUTION FOR THE PRIVACY CHALLENGES IN THE METAVERSE

Attempting to address the matrix of privacy-related challenges discussed above in connection with the *public view*, the following section provides potential insights, which are partially also based on the complex system theory and offers a roadmap for lawmakers to consider.

A. Legal Frameworks, Adaptive Management, and Addressing the Metaverse Complexity

Feedback loops are an integral part of every complex system in which the effects of a change are reflected in the actual cause of that change. In these systems, specific properties develop as a result of the interactions between components and not by summing the individual elements.[261] In a system, individual members and processes are interconnected by complex cause-and-effect relationships, where the state of one influences the form of another.[262] There are many different ways in which feedback loops are a part of our everyday lives.[263] As we interact with others, we are bound to experience both the expected and unforeseen consequences of our actions. Due to these effects, we must adjust our action plans regularly

[258] *See also* Anita L. Allen, Uneasy Access: Privacy for Women in A Free Society (1988) (adopting Gavison's views and argues for extending privacy protection for women); Adam D. Moore, *Privacy: Its Meaning and Value,* 40 Am. Phil. Quarterly 215 (2003) (discussing privacy as a relative right governing the level of control and access to bodies or places of information, which is essential for human flourishing).

[259] Gavison, *supra* note 257 at 423.

[260] *Id*. at 428–436.

[261] John R. Turner & Rose M. Baker, Complexity Theory: An Overview with Potential Applications for the Social Sciences, 7(1) Systems 4 (2019) ("Through emergence, the whole cannot be reduced to the original parts, the whole is considered a new entity or unit… Emergence occurs when the interactions from the system components tend to lead to new states, contributing to the system's unpredictability.").

[262] Paul Plsek, Curt Lindberg & Brenda Zimmerman, Some Emerging Principles for Managers of Complex Adaptive Systems (CAS) 2 (November 25, 1997) ("A system of individual agents, who have the freedom to act in ways that are not always totally predictable and whose actions are interconnected such that one agent's actions change the context for other agents.")

[263] Donella H. Meadows & Diana Wright, Thinking in Systems: A Premier 12–17 (2008).

to ensure they continue to be effective.[264]

Different types of environments, organizations, or institutions resemble the process of complex systems in which information is communicated in two ways across various networks: *Negative and positive feedback forms*.[265] The negative state restricts the outputs produced based on the inputs by creating a response in the opposite direction to a certain one for attaining an overall equilibrium. The positive form reinforces the output based on the input as both move in the same direction and "can permanently push the system in that direction."[266] It is through these loops that the system learns to correct its errors by creating an open-ended process for obtaining and combining information about the effectiveness of its actions so that it can improve its efficiency. Developing such systems requires tolerance for alternative viewpoints, different methods of conducting business, and a willingness to assume risks.[267] Because the feedback loops reflect the interdependencies of various variables with each other, changes to the inputs can have unintended and unanticipated effects on the system's overall conduct. As a result, it is difficult to accurately predict the behavior of complex systems only by referring to a specific input, as multiple players are involved.[268]

As the metaverse exhibits the properties of a complex system, nonlinear feedback effects arising from interactivity between the platforms' users frustrate the ability to predict consequences, such as cause-and-effect explanations for privacy breaches. However, while the metaverse's overall outcomes cannot be predicted easily, this does not necessarily imply that the processes within it cannot be understood.[269] Therefore, policymakers should focus on understanding the interactive patterns and potential feedback effects between players rather than identifying the causal relationship between data violations and damages.[270]

Moreover, the complexity theory suggests abolishing any attempts to control metaverse conduct by directly regulating internal interactions. According to this perspective, data interactions are not reducible to a few rules or "logics" that could govern different actions or simply describe the behavior of the overall systems.[271] Instead, it recommends policymakers create a comprehensive formal legal framework, such as legal principles, laws, and regulatory mechanisms that would induce business entities to self-regulate their structures, operations,

[264] Gökçe Sargut and Rita McGrath, *Learning to Live with Complexity*, Harvard Bus. Rev. (2011), https://hbr.org/2011/09/learning-to-live-with-complexity.

[265] J.B. Ruhl & Daniel Martin Katz, Measuring, *Monitoring, and Managing Legal Complexity*, 101 Iowa L. Rev. 191, 228–231 (2015).

[266] *Id*. at 229.

[267] Justin W. Cook & Piret Tõnurist, From Transactional to Strategic: Systems Approaches to Public Service Challenges 14–15 (OECD, 2016)

[268] Turner & Baker, *supra* note 261 at 8–9.

[269] *Id*. at 13.

[270] Steven L. Schwarcz, *Regulating Complexity in Financial Markets*, 87 Wash. L. Rev. 211, 245–246 (2009)

[271] Volker Schneider, *Governance and Complexity*, in The Oxford Handbook of Governance 129, 139 (David Levi Faur ed., 2012).

and activities.[272] These legal instruments will motivate entities in the metaverse to engage in iterative experimentation of their organizational forms and procedures by exploring the "patterns of interaction that are recognizable across situations to identify an intelligible answer to the question of why something happened in situations where specific causes and effects are not identifiable."[273]

Such inquiry represents the idea of adaptive management. As part of this idea, learning takes place through experimentation by carefully defining goals and developing procedures that undergo regular evaluation and reiteration throughout the process.[274] It "emphasizes learning through management where knowledge is incomplete, and when, despite inherent uncertainty, managers and policymakers must act."[275] Moreover, adaptive management addresses the adjustment of firm-based governance instruments to accommodate the constant changes resulting from the complex environment.[276] To that end, policymakers must design formal laws and government agencies that will stimulate the process of adaptive management.[277] These instruments should be based on the view of facilitating adaptive learning overtime on behalf of the policymakers in a way that would allow them to empirically "track and evaluate results of legal reforms."[278] This will ultimately will result in business entities changing internal governance structures to address privacy challenges in the metaverse effectively.

By engaging in such inquiry,[279] entities are encouraged to modify their internal processes, structure, rules, and procedures to accommodate themselves to the privacy challenges involved in the complex settings of the metaverse.[280] Organizational processes refer to increasing different channels of communication with stakeholders, which could allow taking into account a range of interests and "to assess better the potential and actual challenges."[281] Organizational structures refer to the formation of horizontal or vertical

[272] Dirk Helbing, *Managing Complexity in Socio-Economic Systems*, 17(2) Eu. Rev. 423, 429–433 (2009).

[273] Mary Uhl-Bien & Russ Marion, *Complexity Leadership in Bureaucratic Forms of Organizing: A Meso Model,* 20(4) Leadership Quarterly 631, 637 (2009).

[274] Barbara A. Cosens, J.B. Ruhl, Niko Soininin & Lance Gunderson, *Designing Law to Enable Adaptive Governance of Modern Wicked Problems,* 73 Vanderbilt L. Rev. 1687, 1714 (2020).

[275] Craig R. Allen & Ahjond S. Garmestani, *Adaptive Management*, in Adaptive Management of Social-Ecological Systems 1, 2 (Craig R. Allen & Ahjond S. Garmestani, eds., 2015).

[276] Rika Preiser & Minka Woermann, Co*mplexity, Philosophy and Ethics,* in Global Challenges, Governance, and Complexity: Applications and Frontiers 38, 54 (Victor Galaz ed., 2019).

[277] Cosens et al., *supra* note 274 at 1721–1731.

[278] J. B. Ruhl, Daniel Martin Katz, *Michael J. Bommarito II, Harnessing Legal Complexity*, 355(6332) Science 1377, 1378 (2017).

[279] Martin Reeves, Simon Levin, Thomas Fink & Ania Levina, *Taming Complexity*, Harvard Bus. Rev. (2020), https://hbr.org/2020/01/taming-complexity ("Instead of micromanaging each decision, smart companies realize that allowing individuals the freedom to engage in constant, iterative experimentation can lead to more-powerful outcomes than can deliberately designing and tightly managing each step. This is particularly true in organizations whose environments are evolving in unpredictable and unprecedented ways.").

[280] Anselm Schneider, Christopher Wickert and Emilio Marti, *Reducing Complexity by Creating Complexity: A Systems Theory Perspective on How Organizations Respond to Their Environments*, 54(2) J. of Management Studies 182, 182–184 (2017).

[281] *Id*. at 189.

differentiation. Horizontal differentiation focuses on creating administrative divisions, units, and sub-units, and vertical differentiation relates to establishing several levels of authority and power.[282] A higher number of hierarchical levels is better at handling complex environments because they facilitate more efficient decision-making.[283] Thus, by creating more nuanced organizations and operations, entities are more equipped to meet the challenges of complex surroundings.[284]

As the discussion so far demonstrated, the role of the market solution proposed is to assist government agencies to create regulatory and administrative arrangements that will motivate adaptive management and governance. These practices would allow metaverse entities to independently address data violations in the virtual environments without necessarily assuming liability for specific peer-to-peer privacy breaches. In the next section, we propose a novel arrangement inspired by capital markets law rationales.

B. A Market-Based Approach to Motivate Adaptive Governance for Privacy Protection at the Micro-Level

To induce metaverse entities to engage in adaptive management of their business in the virtual environments and to apply adaptive governance instruments for addressing interconnected data violations, we outline a market-based solution that calls lawmakers to impose mandatory disclosure obligations concerning compliance with data protection regulation and the use of AI.[285] We call for mandate metaverse entities to report how they *internally* address privacy challenges and potential damages in three stages: the *entry, the experience, and the exit stages* within the virtual settings. Various stakeholders and special government agencies will evaluate these immediate and periodic reports to create detailed legal norms and industrial instructions for privacy protection that could motivate metaverse entities' self-regulation.

1. *Market-Based Solution Justifications for Privacy Challenges in the Metaverse*

Mandatory disclosure refers to public companies' obligations to provide information to retail

[282] *Id*. at 188.
[283] *Id*.
[284] *Id*. at 188–189.
[285] The importance of disclosures, certainly in the decentralized, Web3 environment, is a key one, as also discussed by other commentators: "Disclosures should fit the business model, and include an explanation of how and under what circumstances an end user will benefit from using the app. If a dapp's purpose is to enable some form of profit-making, entrepreneurs should take time to explain how earnings are generated. When end users are expected to earn returns. . . or something altogether new like gaming proceeds, entrepreneurs should take the time to explain each concept. Additionally, because such processes may involve third party institutions or processes, they too should be disclosed and explained, along with how earnings are expected to be achieved. If, on the other hand, a dapp is designed to facilitate the purchase of a collectible, or create online communities or games, entrepreneurs should provide a clear overview as to what specifically is being purchased, and how it is accessed. Entrepreneurs should consider disclosing some of the core attributes of the community or social value that the app intends to secure, or what features a particular gaming application will provide for end users." *See* Brummer, *supra* note 109.

investors as part of modern securities law.[286] These obligations are traditionally explained with references to two ideas:[287] *First*, agency cost theory points to the need to redress agency costs between managers and investors by requiring companies to share information on managerial misconduct even if it results in a sharp decline in the stock price.[288] It could deter insider misbehavior since any harmful disclosure may significantly impact managers' reputations.[289] *Second*, there is a concern that public companies will not voluntarily collect and disclose information,[290] especially when "the private benefits of disclosure to issuers may be less than its social benefits to market participants."[291] There could be instances that companies might prefer not to disclose information, "even if investors would want to know it because doing so would aid a competitor."[292] As a result, investors may have difficulty pricing shares accurately based on all available information.[293] By disclosing investment opportunities, investors can compare investment options, and companies can reduce capital costs, thereby allocating resources more efficiently.[294]

Generally, mandatory disclosures are perceived to benefit investors exclusively, while stakeholders are considered indirectly by linking the sharing of valuable information to promoting market functions. However, recently, scholars called to extend the mandatory information sharing also to important stakeholders. Ann Lipton argued that extending corporate transparency to stakeholders could serve several functions.[295] For example, disclosures may benefit a variety of constituencies, such as employees, creditors and suppliers who have contractual relationship with the company and are fixed claimants.[296] They can use this information before engaging with the company or when they decide on renewing previous connections under certain terms.[297] Moreover, by sharing information with various constituencies, stakeholders can discipline corporate conduct in a way that is

[286] Andrew A. Schwartz, *Mandatory Disclosure in Primary Markets*, 2019 Utah L. Rev. 1069, 1069–1072 (2019).
[287] *Id*. at 1081–1087.
[288] Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 Wash. U. L. Q. 417, 463 (2003) ("The argument is that disclosure has a prophylactic effect by deterring corporate insiders from engaging in fraudulent or corrupt behavior or mismanagement").
[289] Schwartz, *supra* note 286, at 1071.
[290] Reinier R. Kraakman, et al., The Anatomy of Corporate Law: A Comparative and Functional Approach 246 (3rd ed., 2017) ("The case for mandatory disclosure that firms will not disclose sufficient, or sufficiently comparable, information without it."); Luca Enriques & Sergio Gilotta, *Disclosure and Financial Market Regulation*, in Oxford Handbook on Financial Regulation 514 (Niamh Moloney, Eilís Ferran, and Jennifer Payneeds eds., 2015).
[291] Kraakman, *Id*.
[292] Schwartz, *supra* note 286 at 1087.
[293] *Id*. at 1086.
[294] John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 Va. L. Rev. 717, 734 (1984).
[295] Ann M. Lipton, *Not Everything Is about Investors: The Case for Mandatory Stakeholder Disclosure*, 37 Yale J. on Reg. 499 (2020).
[296] *Id*. at 511.
[297] *Id*. at 511–513.

compatible with social responsibility principles.[298] In addition to enhancing the informational setting in which lawmakers function, a public disclosure system makes regulation more effective.[299] It allows the public to play a more active part in the regulatory process, resulting in bottom-up regulatory changes that are more sensitive to society's demands, especially when it comes to entities that provide essential services.[300] In a similar vein, Stephanie Bornstein argued that lawmakers should impose public disclosure requirements on employers to enforce antidiscrimination laws better.[301] Her proposal is to create a disclosure system that would track decisions about employee pay, promotions, and harassment based on sex and race considerations.[302]

We believe that imposing on metaverse entities privacy-related mandatory obligations that are subject to regulatory review and inputs will motivate the formers to self-regulate their operations and setups. It is essential, however, to introduce these mandatory obligations with complementary liability regimes that are activated when either: (i) the entities provide partial or misleading disclosures regarding how their AI systems protect the privacy rights of their users; or (ii) the information provided by the entities indicates that their infrastructures do not provide sufficient or effective safeguards against data violations. To avoid potential liability that would have serious financial consequences, metaverse entities are more likely to alter their AI infrastructures and governance practices to ensure users are safe.

2. *Models for Mandatory Disclosure of Privacy on Metaverse Entities*

We suggest imposing on metaverse entities disclosure obligations on privacy protections that they provide to users as part of building, sustaining, and developing the virtual infrastructures. We distinguish between different stages of communications: entry, experience, and exit.[303] Several scholars have already suggested to impose transparency obligations on digital platforms that would enable regulatory agencies to address cases of personalization-driven harms.[304] Previous proposals focused on how such obligations can reinforce enforcement actions "against problematic personalization – criminal or civil penalties for platforms; flagging, deprioritizing, or blocking of content reflecting problematic personalization."[305] However, as described below, our proposal refers to imposing privacy mandatory disclosure obligations that will induce metaverse entities to self-regulate their AI systems to ensure privacy protection to users.

a. Entry

[298] *Id*. at 513–517.
[299] *Id*. at 517–519.
[300] *Id*. at 518–519.
[301] Stephanie Bornstein, Disclosing Discrimination, 101 B.U. L. Rev. 287 (2021).
[302] *Id*. at 300–313.
[303] *See e.g.,* Ayelet Gordon-Tapiero, Alexandra Wood & Katrina Ligett, *The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization*, Vanderbilt J. of Ent. & Tech. L. (2023).
[304] *Id*. at 40–47.
[305] *Id*. at 66.

Privacy policies are traditionally perceived as the primary defense provided to users by states, platforms and business entities concerning the collection, share and use of personal information with third parties.[306] However, scholars have extensively discussed why these terms and conditions do not provide meaningful protection to users when they are considered from contract and privacy laws perspective.[307] Contract law scholars explained that consumers generally do not understand privacy terms and therefore consider them to be practically incomprehensible,[308] making it difficult for business entities to communicate their privacy practices in a way that will attract consumers' attention.[309] Moreover, it was demonstrated that even simplifying disclosures will not necessarily enhance consumer understanding.[310]

These terms are described as excessively long, using language difficult for the average person to understand.[311] Additionally, even when opting out of intrusive data practices is explicitly included in the contract, consumers find it difficult to do so. Consequently, most consumers don't read privacy terms, especially since doing so is rational.[312] From a privacy law perspective,[313] researchers argued that firms receive consumer consent by using "dark patterns" to induce consumers into accepting terms without having ever read or understood them.[314] In dark patterns, designers are deliberately manipulating users in such a way that

[306] Thomas Haley, *Illusory Privacy*, 98(2) Indiana L. J. 75, 88 (2022) ("Platform terms are everywhere. They gatekeep access to daily computing necessities like Google's and Microsoft's suites of services. Unfortunately, they are also the primary line of defense between a person's private information and how a platform can use it.").

[307] *See* also, Joseph Turow, Yphtach Lelkes, Nora A. Draper & Ari Ezra Waldman, *American Can't Consent to Companies' Use of their Data* 17 (Annenberg School for Communication - University of Pennsylvania, 2023) (finding "that overwhelmingly and to an extent not known before, Americans neither understand commercial surveillance practices and policies nor feel they are capable of doing anything about rampant data extraction.").

[308] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. Rev. 647, 665–672 (2011) (Showing why in the context of boilerplate consumer contracts, mandated disclosure is not an effective policy tool)

[309] *Id*. at 87–94; Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. Legal Stud. S69, S87 (2016) (indicating there was no difference between terms that had been determined to be legally problematic and those that had been found to be enforceable);

[310] Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. Legal Stud. S41, S65–66 (2016)

[311] Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 Info., Commc'n & Soc'y 128 (2020) (reporting the results of an experimental survey indicating that individuals ignored privacy policies (PP) and terms of conditions (TOS) when joining a fictitious social networking service. In the study, information overload was found to be a significant negative predictor of reading the TOS upon signing up, when the TOS changes, and when the PP changes).

[312] *See e.g.,* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 Harv. L. Rev. 2010, 2026 (2013) (arguing that people do not care about their own privacy and cannot understand those individuals who do care about privacy).

[313] *See e.g.*, Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law* (Jan. 22, 2023), https://ssrn.com/abstract=4333743 (arguing that privacy consent is fictitious and in most cases, people are ill-equipped to make decision about privacy. Therefore, law should adopt a middle ground approach between full consent and non-consent which the author terms as "murky consent.")

[314] Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 Current Opinion in Psychology 105, 105–107 (2020).

they attempt to confuse them into agreeing to certain actions that are not in their interests. For example, they may convince them to purchase goods and services they are not interested in or to share personal data they would prefer to remain anonymous.[315] In a recent study, Jamie Luguri and Lior Strahilevitz report on the results of large-scale experiments on dark patterns imposed on a representative sample of American consumers.[316] Users exposed to mild dark patterns were twice as likely as those assigned to a control group to sign up for dubious services. However, users in the aggressive dark state were almost four times as likely to subscribe.[317] Significantly, low-educated subjects were more susceptible to mild dark patterns than those with higher education.[318] The results indicate that consumers' consumption decisions are largely influenced by the architectural context in which they make their decisions rather than the price of the products or services they select.[319]

Taking these concerns seriously, we believe that the infrastructures of the metaverse themselves should be employed to create privacy policies that are communicated to users effectively. Particularly, with a virtual setting, users would be able to visualize privacy policies without having to read the terms beforehand and understand their content. To illustrate this idea, consider metaverse data violations as types of potential aviation accidents, and to avoid them, entities should demonstrate *visually* how they are taking steps to prevent them.[320] However, to make this mechanism successful, entities will have to provide comprehensive information to a certain regulatory agency on how they have visually communicated their privacy terms and conditions to their users before entering to the metaverse and how the imagining can be improved in a way that takes into account different potential data violation in the virtual environments.[321]

b. Experience

As discussed earlier,[322] collecting, using, and sharing personal data is crucial to creating fully immersive experiences. Consequently, it is regarded as an essential part of the metaverse's

[315] *Id*.
[316] Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns,* 13 J. of Legal Analysis 43 (2021).
[317] *Id*. at 64.
[318] *Id*. at 70–71.
[319] *Id*. at 98; Brummer*, supra* note 109. Also *see generally* Elizabeth M. Renieris, Beyond Data: Reclaiming Human Rights at The Dawn Of The Metaverse (2023).
[320] *See e.g.,* Wentao Guo, Jay Rodolitz & Eleanor Birrell, Poli-see: An Interactive Tool for Visualizing Privacy Policies, Proceedings of the 19th Workshop on Privacy in the Electronic Society (2020), https://dl.acm.org/doi/abs/10.1145/3411497.3420221.
[321] Lie et al. made a related proposal to ours. The researchers examined how to improve the usability of privacy policies in relation to their role in enabling meaningful accountability. Specifically, they argue that privacy policies should be viewed as dynamic transparency tools that enable meaningful accountability. The authors examine how an automated privacy policy analysis focused on data flows can identify apps that mishandle personal information. *See*, David Lie, Lisa M. Austin, Peter Yi Ping Sun & Wenjun Qiu, *Automating Accountability? Privacy Policies, Data Transparency, and the Third-Party Problem*, 72(2) Toronto L. J. 155 (2022).
[322] *See* Section III Part A and B.

AI infrastructure.[323] AI design and applications can generate different types of algorithmic harm. In general, machine-learning algorithms are inherently linked to the quality of the data that is used to develop them, and poor or deficient inputs can result in serious social distortions.[324] An example of this is when the data used to develop a machine-learning algorithm is biased and reflects previous prejudices or inequalities.[325] Moreover, the promise of AI decision-making is also somewhat offset by the fact that it can contribute to systemic social injustices. One such serious harm is termed "proxy discrimination."[326] An algorithmic system engages in proxy discrimination when it employs one or more seemingly neutral variables to capture legally protected characteristics, often causing protected groups to be treated differently in terms of economic, social, and political opportunities.[327] To put it simply, these algorithms identify a set of neutral characteristics so as to create groups that closely resemble protected classes, and these "proxies" are used to include or exclude certain disadvantaged socio-economic groups.[328] There is already evidence that minorities and people of color suffer from a variety of biases in the online environment and digital economy, manifested in discriminatory oversurveillance, discriminatory exclusion, and discriminatory predation.[329] In the AI virtual spaces of the metaverse, such discrimination could, however, be significantly exacerbated, resulting in an even more tolling systemic particularly to socioeconomically disadvantaged groups. Therefore, any tools that would prove effective in improving AI systems' fairness would be very much needed.

Therefore, we argue that privacy mandatory disclosure obligations can be used to improve AI systems' fairness. Specifically, by subjecting metaverse entities to privacy disclosure on their AI infrastructures, regulatory agencies would be more equipped to instruct them how to correct AI functions by removing gender or race biased data from the algorithm.[330] Furthermore, sharing information would allow agencies to guide the creation of AI infrastructures that utilize noise in the algorithms to efficiently debias data inputs to achieve justice and fairness.[331] An example for such practices is synthetic data, which is a computer-

[323] *Id*.

[324] Rebecca Kelly Slaughter, Janice Kopec & Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission,* 23 Yale J. L. & Tech. 1, 6–37 (2021); Andrew D. Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. Pennsylvania L. Rev. 9–27 (2023).

[325] Slaughter et al., *supra* note 324 at 7–8.

[326] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data,* 105 Iowa L. Rev. 1257 (2020)

[327] *Id*. at 1260–61, 1269–1270, 1273.

[328] Slaughter et al., *supra* note 324, at 20–24.

[329] Anita Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907 (2022) (discussing the discriminatory oversurveillance, discriminatory exclusion and discriminatory predation African Americans face online).

[330] Michael Selmi, *Algorithms, Discrimination and the Law*, 82(4) Ohio State L. J 611, 630–632 (2021).

[331] *See* generally Bo Cowgill, *Bias and Productivity in Humans and Machines* 1–8 (Upjohn Inst., Working Paper No. 19-309, 2019), https://ssrn.com/abstract=3433737. *See also*, Thomas Nachbar, *Algorithmic Fairness, Algorithmic Discrimination,* 48 Florida State L. Rev. 509 (2021) (For algorithmic decision-making to be

generated data that is designed to mimic real-world data.[332] It can be used with AI tools to address biases in algorithms by providing a larger, more diverse dataset that can be used to train machine learning models.[333] Synthetic data is beneficial because it allows for the inclusion of more data points, which can help reduce the potential for bias in algorithms.[334] Additionally, synthetic data can be used to fill in gaps in existing datasets, allowing for a more comprehensive picture of the data.[335] This can help to reduce the risk of bias, as well as provide more accurate results when using AI tools and algorithms. Therefore, by adopting clear transparency mechanisms, discriminative results could be reduced and affirmative actions could be applied to promote the rights and interests of underprivileged populations.[336]

c. Exit

Since the metaverse system is based on algorithmic decision-making mechanisms that could cause privacy damages,[337] the law should allow individuals affected by AI decisions the right to contest those decisions.[338] By providing users with a fundamental right to challenge the metaverse's AI outcomes according to clearly regulated processes, the law can incorporate procedural and sustainable fairness considerations within any individual data relationship.[339] Since statutory dispute mechanisms do not cover most online content, many platforms have implemented contestation schemes governed only by their preferences.[340] For example, in 2018 Meta established the Oversight Board (OB) as an independent institution reviewing Facebook and Instagram’s content moderation decisions.[341] However, the OB was “not designed to be a simple extension of (Meta’s) existing content review process” but rather to “review a selected number of highly emblematic cases and determine if decisions were made

corrected, it Is necessary to break down the process into two separate decisions: rejecting old processes and adopting new ones).

[332] Alex LaCsse, *Synthetic data a key to privacy by design practices in new Canadian smart city partnership Schedule,* IAPP (Nov. 29, 2022), https://iapp.org/news/a/synthetic-data-is-key-to-privacy-by-design-practices-in-new-canadian-smart-city-partnership/

[333] Michal Gal, *Synthetic Data: Competitive and Human Dignity Implications* (forthcoming: 2023), https://www.dli.tech.cornell.edu/seminars/Synthetic-Data%3A-Competitive-and-Human-Dignity-Implications (arguing that “it is forecasted that by 2024, 60% of data used to train artificial intelligence systems around the world will be synthetic”)

[334] Gal, *supra* note 333. *See also* Alice Xiang, *Being 'Seen' vs. 'Mis-Seen': Tensions between Privacy and Fairness in Computer Vision*, 36 Harvard J. of L. & Tech, (forthcoming), at https://ssrn.com/abstract=4068921 or http://dx.doi.org/10.2139/ssrn.4068921

[335] Gal, *supra* note 333.

[336] Nachbar, *Id*. at 548–556.

[337] *See e.g.,* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 Boston University Law Review 793, 830– 861 (2022).

[338] Margot E. Kaminski and Jennifer M. Urban, *The Right to Contest AI*, 121 Colum. L. Rev. 1957, 1965–1988 (2021).

[339] *Id*. at 1994–2003.

[340] *Id*. at 2011.

[341] *See* Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression,* 129 Yale L.J. 2418 (2020) (examining the motivations behind Facebook's decision to create the Oversight Board and its implications for internet governance and global freedom of expression).

in accordance with [Meta's] stated values and policies."[342] It focuses particularly on "the impact of removing content in light of human rights norms protecting free expression" balanced against other values such as "authenticity, safety, privacy and dignity."[343] The OB can impact Facebook and Instagram's content moderation in several manners. For example, it upholds or overturns Meta's moderation decision. Meta is obligated to adhere to the OB's ruling, unless doing so would violate the law in a given jurisdiction.[344] Furthermore, the OB's past decisions may also serve as precedents for future decisions regarding content moderation that share similar factual patterns. Specifically, OB's rulings can serve as precedents "for deciding subsequent cases involving identical or similar facts, or similar legal issues."[345] We believe that each metaverse entity should set up an independent body for resolving disputes with users. Specifically, these institutions must address potential data violations and discriminatory AI outcomes that result in personal or social harms within or outside the virtual environment. The effectiveness of these independent bodies could be enhanced by requiring the metaverse entities to disclose details not only about institutions' resolutions but also any relevant information that could affect users' right to contest, such as governance, functions, and procedures. In our opinion, mandatory disclosure can motivate the metaverse's entities to improve their private contestation policies and mechanisms to reduce the risk of liability for partial, misleading or ineffective disclosure obligations. This will allow users to protect their data effectively by subjecting the operations of these independent bodies to periodical regulatory examination and supervision.

CONCLUSION

This Article is a primary and novel attempt to support the development of a safer and more privacy-friendly metaverse. Following our multi-level conceptualization of data exchanges in the virtual space, we argued that traditional privacy law cannot provide sufficient protection against data violations. Therefore, to enhance privacy in the micro-level, we proposed adopting a market for privacy mandatory disclosure obligations, envisaging a scheme whereby metaverse entities share comprehensive information with regulatory authorities on the protection they afford to users' privacy. The regime proposed will motivate metaverse entities to self-regulate their AI systems to guarantee valuable protection. Furthermore, we believe that studying how Web3 differs from Web2 under the *public* view is worthwhile because it could alter the fundamental principles that lay at the intersection of law, technology, and the business environment, similar to the Internet before it.[346] Since

[342] David Wong & Luciano Floridi, *Meta's Oversight Board: A Review and Critical Assessment*, Minds and Machines 3 (2023), https://link.springer.com/article/10.1007/s11023-022-09613-x.

[343] *Id.*

[344] *Id*. at 4.

[345] *Id.*

[346] This relates to an older debate on whether studying the law of the cyberspace is valuable. For more on the policy debate around the term the "law of the horse," which was coined by Judge Frank Easterbrook in connection with the law of cyberspace, arguing that the law of cyberspace is only a specialized endeavor to which general legal rules could be applied as problems arise on a case-by-case basis, instead of a separate,

Web3 marketplaces are presently created, our investigation allows unleashing their economic value, creating sustainable virtual spaces and providing meaningful safeguards to privacy rights of individuals, populations and groups.

distinct area of law. *See* Frank H. Easterbrook, *Cyberspace, and the Law of the Horse,* 1996 U. Chi. L. F. 207, 207 ("[T]he best way to learn the law applicable to specialized endeavors is to study general rules."). *cf.* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 502 (1999) ("[T]here is an important general point that comes from thinking in particular about how law and cyberspace connect.").